21世纪高等院校计算机网络工程专业规划教材

网络管理技术教程

陈广山 编著

清华大学出版社

21 世纪高等院校计算机网络工程专业规划教材

网络管理技术教程

陈广山　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书首先介绍了网络管理的基础知识，包括网络管理的基本概念、要素、目标、内容、功能、模型和标准，管理信息库，简单网络管理协议，以及远程网络监视 RMON；然后介绍了常用网络设备，包括常用服务器、交换机、路由器和电源等设备的管理；接下来介绍了 IT 运维和安全管理的相关内容，包括日常运维管理、信息安全管理和网络管理系统；最后介绍了网络管理工具和故障诊断与维护的知识。

全书力求体现实际、实用的原则。这是一本具有可操作性的网络管理教程，书中所选软件，大多可从网上免费下载试用，或直接在网上体验。全书理论体系相对完整，采用了尽可能多的实际操作案例来解释和阐述相应的具体应用，每章配有习题，供读者巩固学到的知识和技能。

本书可作为本、专科“计算机网络管理”类课程的教材，也可作为相关培训班的教程，同时还可作为网络管理人员的参考书。

图书在版编目(CIP)数据

网络管理技术教程/陈广山编著. —北京：清华大学出版社，2011.8
(21 世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-25082-1

Ⅰ. ①网…　Ⅱ. ①陈…　Ⅲ. ①计算机网络管理—高等学校—教材　Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字(2011)第 046529 号

责任编辑：梁　颖
责任校对：白　蕾

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：
经　　销：全国新华书店
开　　本：185×260　　**印　张**：18.5　　**字　　数**：449 千字
版　　次：2011 年 8 月第 1 版　　**印　　次**：2011 年 8 月第 1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：035902-01

前　　言

随着设备的增多，网络规模的扩大，网络管理的负担正在进一步加重。而且，随着企业的业务变得越来越富有挑战性，作为支撑业务的网络管理工作也变得越来越复杂。如何优化设备和网络配置，使网络系统充分发挥优势，是网络管理员们正面临的艰巨任务。网络管理是业务运营中的一个关键环节，网络管理的质量也会直接影响网络的运行效率和企业的效益。因此，实现有效的网络管理，促进网络安全、稳定地运行就显得越来越重要，同时对网络管理者的素质要求也越来越高。因此，编者从实际应用的需求出发，结合多年从事网络管理教学和工作的经验编写了本书。

本书共分为 9 章，每章都配有习题。在编写的过程中注意到了作为教材其理论体系的完整性和实验的可操作性，几乎所有软件都可从网上免费下载，或直接在网上体验。

第 1 章介绍网络管理的基础知识，包括网络管理的概念、要素、目标、内容、功能、模型和标准；第 2 章介绍管理信息库；第 3 章介绍网络管理协议，主要介绍 SNMP 协议的发展、功能、体系结构，以及公共管理信息协议和基于 Web 的管理技术；第 4 章简单介绍远程监视 RMON 的相关内容；第 5 章介绍服务器、交换机、路由器、电源等常用网络设备的配置与管理；第 6 章介绍日常运维和管理的内容和操作，包括企业网站设计与管理，网络布线和数据库管理，软硬件资源管理，业务和文档的管理等；第 7 章介绍信息安全管理的基本知识，主要有环境安全、数据存取管理和容灾管理；第 8 章介绍常用网络管理工具和企业级网络管理系统；第 9 章介绍网络故障诊断与维护的相关理论知识、技术、手段、方法和技巧。

在本书编写的过程中参考了大量的文献，在此对相关的作者表示感谢；同时也得到编者所在单位的领导和许多老师的帮助，以及实验中心全体同仁的支持，在此也表示衷心的感谢！

由于编者水平有限，难免会有错误和不足，敬请专家和读者批评和指正。

编者

2011 年 5 月

目　录

第1章 网络管理基础

计算机网络技术已经历了将近50年迅速发展的过程。今天,计算机网络作为信息社会的基础设施已经渗透到社会的各个方面,政府部门、商业、军事、教育和科研等领域都离不开计算机网络。社会对计算机网络的依赖,使得计算机网络本身运行的可靠性越来越重要。目前的计算机网络规模已经越来越大,组成也越来越复杂,人工网络管理的方式已经无能为力,因此对网络运行的管理提出了更高的要求。

1.1 网络管理的基本概念

1.1.1 网络管理研究概述

实际上,任何一个系统都是需要管理的,无论是电信网络,还是计算机网络。只是根据系统的大小、复杂性的高低,管理在系统中的重要性有重有轻而已。对计算机网络管理而言,可以说是伴随着1969年世界上第一个计算机网络——ARPANET的诞生而产生的,当时的ARPANET已经存在一个网络管理系统。虽然网络管理技术很早就有,却一直没有得到应有的重视。随着网络的发展,规模增大、复杂性增加,以前的网络管理技术已经不能适应网络的迅速发展了。

20世纪80年代初期,Internet的出现和发展更使人们意识到网络管理的重要性。于是,研究开发人员迅速展开了对网络管理的研究,并提出了多种网络管理方案,包括HEMS、SGMP、CMIS/CMIP等。到1987年底,Internet的核心管理机构IAB意识到需要在众多的网络管理方案中进行选择,以便集中对网络管理的研究。IAB要选择适合于TCP/IP网络特别是Internet的管理方案。在1988年3月的会议上,IAB制订了Internet管理的发展策略,即采用SGMP作为短期的Internet管理解决方案,并在适当的时候转向CMIS/CMIP。其中,简单网关监视协议(Simple Gateway Management Protocol,SGMP)是在NYSERNET和SURANET上开发应用的网络管理工具,而CMIS/CMIP是20世纪80年代中期国际标准化组织(ISO)和CCITT联合制订的网络管理标准。同时,IAB还分别成立了相应的工作组,对这些方案进行适当的修订,使它们更适合Internet的管理。

这些工作组随后相应推出了简单网络管理协议(Simple Network Management Protocol,SNMP)(1988)和CMOT(CMIP/CMIS Over TCP/IP)(1989)。SNMP一推出就得到了广泛的应用和支持,而CMIS/CMIP的实现却由于其复杂性和实现代价太高而遇到了困难。当ISO不断修改CMIP/CMIS使之趋于成熟时,SNMP在实际应用环境中得到了检验和发展。1990年IETF在RFC1157中正式公布了SNMP,1993年4月又发布了

SNMP v2(RFC1441)。当ISO的网络管理标准终于趋向成熟时,SNMP已经得到了数百家厂商的支持,目前SNMP已成为网络管理领域中事实上的工业标准,大多数网络管理系统和平台都是基于SNMP的。

由于实际应用的需要,IEEE通信学会下属的网络营运与管理专业委员会(CNOM),从1988年起每两年举办一次网络营运与管理专题讨论会(NOMS)。国际信息处理联合会(IFIP)也从1989年开始每两年举办一次综合网络管理专题讨论会。还有一个OSI网络管理论坛(OSI/NMFORUM),专门讨论网络管理的有关问题。近几年来,又有一些厂商和组织推出了自己的网络管理解决方案,各大计算机与网络通信厂商也推出了各自的网络管理系统,如HP的OpenView、IBM的NetView等,它们都已在各种实际应用环境中得到了一定的应用,并已有了相当的影响。

1.1.2 网络管理的需求

从用户的角度讲,一个网络管理系统应该满足以下要求。

1. 同时支持网络监视和控制两方面的能力

网络监视功能是为了掌握网络运行的实时状态;而网络控制功能是采取措施影响网络的运行状态。许多网络管理功能同时包含这两方面的能力,例如,在故障管理中,网络监视能力用来发现和诊断网络故障,网络控制能力用来分离故障、定位故障、最终排除故障。

2. 能够管理所有的网络协议

现代网络体系结构是分层设计的,网络的功能和完成功能的协议也是分层的,不同层次的协议完成不同的功能,也可能处于不同的运行状态,因此通用的网络管理系统应该能够管理网络中尽可能多的协议层。

3. 尽可能大的管理范围

在管理尽可能多的网络协议层的同时,还应该考虑扩大网络管理的范围;不仅管理点到点的网络通信,还应管理端到端的网络通信;不仅管理基本的网络设备,还应该具有管理应用的功能。

4. 尽可能小的系统开销

管理尽可能多的协议层和尽可能大的范围肯定是以增大系统开销为代价的,所以网络管理系统应该根据实际情况对网络管理的范围和所需系统开销作一个统一的、合理的分配和选择。在网络管理任务不打折扣的前提下,尽可能减少系统开销,提高网络的运行效率。而且,由于网络管理系统的运行会增加网络的额外流量,所以,减少系统开销的另一个方面就是用于实现网络管理的带宽开销必须合理。

5. 可以管理不同厂家的连网设备

现代大型计算机网络一般是由不同厂家提供的设备连接而成的,网络管理和运行应该不受具体厂家设备的限制。

6. 容纳不同的网络管理系统

大型计算机网络一般可能连接不同的地区或局域计算机网络,这些网络可能具备各自不同的网络管理功能。而尽可能容纳不同的管理功能,形成全网统一的网络管理和运行机制是十分重要的。

7. 网络管理的标准化

管理不同厂家的连网设备和容纳不同的网络管理系统一般应该通过网络管理的标准化来实现。ISO 十分重视网络管理的标准化工作，制定了一系列的网络管理标准。Internet 在实践中已形成了一整套的网络管理工业标准，网络管理系统的设计和运行应该采用标准化的网络管理机制和协议。

1.1.3 网络管理的概念

一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。国际标准化组织在 ISO/IEC7498—4 中定义并描述了开放系统互连(OSI)管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互连管理是指这样一些功能，它们控制、协调、监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。

1. OSI 管理框架

OSI 系统管理操作在对等的开放系统之间进行，一个系统为管理者，另一个系统起代理的作用，即管理者实施管理功能，而代理接受管理者的查询，并且根据管理者的命令设置管理对象的参数。

管理者和代理要能够互相通信，它们之间就要互相了解，这可以通过交换应用上下文(Application Context，AC)实现。AC 是指管理者和代理之间共同使用的应用服务元素及其调用规则。至于具有哪些功能和功能单元，支持哪些管理对象类，管理功能和管理对象之间有什么关系等，也是彼此需要了解的，这些叫做共享的管理知识。系统管理应用实体的管理知识存储在本地的文件中，在应用联系建立阶段，通过交换应用上下文，形成共享的管理知识。

2. 通信机制

管理者和代理间的信息交换是通过协议数据单元(PDU)进行的。通常是管理者向代理发送请求 PDU，代理以响应 PDU 回答，而管理信息包含在 PDU 参数中。在有些情况下，代理也可能向管理者发送消息，通常把这种消息叫做时间报告(或通知)，管理者可根据报告的内容决定是否作出回答。

为了及时了解管理对象的最新情况，代理必须经常地查询对象的各种参数，这种定期查询叫做轮询(Polling)。轮询的间隔或频度对于网络管理的性能有很大的影响。轮询过于频繁，会加重网络通信负载；轮询稀少，又不能及时掌握管理对象的最新状态，所以轮询的间隔应根据网络配置和管理标准仔细设计。另外，如果管理对象中出现了特殊情况，管理对象不必等待代理查询，可直接向代理发出通知。如果必要，代理可以把对象的通知以事件报告的形式发往管理者。

有时管理者想知道代理是否存在，是否可随时与之通信。这时可以利用一种叫做“心跳”(Heartbeats)的机制，即代理每隔一定时间向管理者发出信号，报告自己的状态。同样，“心跳”的间隔也是需要慎重决策的。

3. 管理域和行政域

对于分布式管理，管理域是一个重要的概念，管理对象的集合叫做管理域。管理域的划分可能是基于地理范围的，也可能是基于管理功能的，或者是基于技术的原因。无论怎样划分，其目的都是对于不同管理域中的对象实行不同的管理策略。

每个管理域有一个唯一的名字，包含一组被管理对象，代理和管理对象之间有一套通信规则。属于一个管理域的对象也可能属于另一个管理域，当网络被划分为不同的管理域后，还应该有一个更高级的控制中心，以免引起混乱。因而在以上概念模型的基础上又引入行政域的概念。行政域的作用是划分和改变管理域，协调管理域之间的关系。此外，行政域也对本域中的管理对象和代理实施管理和控制。

4. 管理信息结构

管理信息描述管理对象的状态和行为，OSI 标准采用面向对象的模型定义管理对象。按照对象类的继承关系，表示管理信息的所有对象类组成一个继承层次树。设计一个新的对象类时不必全部从头开始，可以根据新数据类型的属性和已有对类的相似关系把新类插入到继承层次树中。相同的属性可以从父类中继承，再在父类的基础上设计新对象类的特性，从而减少了设计工作量。

OSI 管理的面向对象模型是一个非常复杂的模型，几乎囊括了已知的所有面向对象的概念，例如多继承性、多态性和同质异晶性等。多继承性是指一个子类有多个超类；多态性源于继承性，子类继承超类的操作，同时又对继承的操作做了特别的修改，这样不同的对象类对同一操作会做出不同的响应，这种特性就叫做多态性；同质异晶性是指一个对象可以是多个对象类的实例，例如，一个协议有两个兼容版本，一个协议实体既是老版本的实例，又是新版本的实例。

一个管理对象可以是另一个管理对象的一部分，这就形成了管理对象之间的包含关系。包含关系可以表示成有向的包含树。包含树与对象名的命名有关，因而包含树对应于对象命名树。对象的名字分为全局名和本地名。全局名从包含树的树根开始，向下级联各个被包含对象的名字，直到指称的对象；而本地名则可以从任意上级包含对象的名字开始向下级联。

5. 系统管理支持功能

简单地说，应用层由应用进程（Application Process，AP）及其使用的应用实体（Application Entity，AE）组成，应用进程把信息处理功能和通信功能组合在一起，通过一个全局的名字可以调用这个功能。应用进程的通信功能是由应用实体实现的。为了实现不同性质的通信，一个应用进程可能使用一个或多个应用实体。应用实体还可以再划分为应用服务元素（Application Service Element，ASE）。ASE 是具有简单通信能力的功能模块，对等的 ASE 之间有专用的服务定义和协议规范。应用实体首先要与对等的应用实体建立应用联系（Application Association，AA），然后才能通信。建立应用联系的过程主要是交换 AC。AC 是可以用名字（对象标识符）引用的一组 ASE 及其调用规则，在建立联系期间通过协商确定共同认可的 AC，并在应用活动期间遵守商定的通信规则。

应用服务元素分为公用服务元素和专用服务元素。在网络管理中使用的公用服务元素有联系控制服务元素（ACSE）和远程操作服务元素（ROSE）。ACSE 专门用于建立应用联系，这个元素对任何应用都是必要的；ROSE 用于实现对等应用实体之间远程过程调用，当

管理者启动管理对象中的特殊操作时要利用这个元素。网络管理中使用的专用服务元素叫做公共管理信息服务元素(CMISE),这一组服务元素共同组成公共管理信息服务(CMIS),在 OSI 管理标准中,公共管理服务元素和公共管理协议操作一一对应。

1.2 网络管理的基本要素

网络管理需要能够监视和控制网络中的各种物理介质和连网设备、计算机设备、网络互联设备、操作系统软件等各种硬件、固件和软件元素资源。其基本要素主要包括 3 个方面:网络管理对象、网络管理方法和网络管理系统。

1. 网络管理对象

网络管理对象可以理解为网络管理的环境,它主要有以下 4 类。

(1) 网络信号传输系统:网络信号传输系统是指网络信号传输系统所涉及的各类物理设施,如网络传输介质等。

(2) 网络节点设备:网络节点设备是指计算机网络中的主机(服务器)、工作站、网桥、网关、路由器、交换机、提供智能业务的控制点(如硬件防火墙等)、广域网的接入设备、信令设备等。

(3) 网络间的联系:网络上各种设备要按照一定的方法建立相应的联系,这种联系实际上描述了网络上设备之间的关系,这种关系就形成了网络。通常所说的网络,都是指网络上的节点和节点设备间的某种关系。

(4) 网络上的业务:网络能够提供各种服务,表现为网络用户(工作站)上的具体业务应用。作为网络管理对象、业务、网络和网络上的节点设备,在形态上有很大的区别。网络上的节点设备是物理意义上存在的实体。网络间的关系不像节点设备有明显的物理存在特征,但网络用户可以通过业务节点设备和传输设备感受到。

2. 网络管理方法

网络管理方法根据划分的标准,可以分为很多种,以下是一些常用网络管理方法的分类:

(1) 根据网络管理的分布或集中,可分为基于分布管理的网络管理方法和基于集中管理的网络管理方法。

(2) 根据网络管理环境,可以分为面向狭义的网络管理环境的网络管理方法和面向广义的网络管理环境的网络管理方法。

(3) 根据是否具有智能特征,可以分为智能化的网络管理方法和常规性的网络管理方法。

(4) 根据采用网络管理标准的程度,可分为基于标准的网络管理方法和基于非标准的网络管理方法。

3. 网络管理系统

网络管理系统是指在网络管理环境中实现网络管理方法的计算机应用系统,如 IBM 公司开发的 Tivoli NetView 网络管理系统、HP 公司开发的 OpenView 网络管理系统、锐捷网络公司开发的 StarView 网络管理系统等。

1.3 网络管理的目标和内容

1. 网络管理的目标

网络管理的目标就是最大限度增加网络的可用性，合理组织和配置系统资源，提供安全、可靠、有效和优质的服务，保证网络正常、经济、可靠和安全地运行。或者说网络管理的目标就是对网络资源进行合理分配和控制，以满足业务提供者的要求和网络用户的需要，使网络资源得到最大限度的利用，使整个网络更加经济地运行，并同时提供连续、可靠和稳定的服务。主要包括以下几方面：

- 减少停机时间，改进响应时间，提高设备利用率。
- 减少运行费用，提高效率。
- 减少/消灭网络瓶颈。
- 适应新技术(多媒体、多种平台)。
- 使网络更容易使用。

2. 网络管理的内容

现代网络管理的内容通常可用运行、控制、维护和提供加以区分，概括为以下几方面。

- 运行：针对网络用户提供的服务而开展的、面向网络整体进行的管理活动，如用户管理和用户计费等。
- 控制：针对网络用户提供的有效服务、为满足服务质量要求而进行的管理活动，如对网络流量的管理。
- 维护：针对保障网络机器设备的正常、可靠、连续运行而进行的活动，如故障的监测、定位和排除。维护可分为预防性维护和修正性维护。
- 提供：针对网络资源的服务而进行的管理活动，如安装软件、配置各类参数等，为实现某个服务而提供资源、向用户提供某项服务等。

1.4 网络管理系统的功能

1.4.1 故障管理

故障管理(fault management)是网络管理中最基本的功能之一。每个用户都希望自己有一个可靠的计算机网络，当网络中某个部分失效时，网络管理系统能够迅速地查找到故障并及时排除。通常迅速隔离某个故障是不大可能的，因为网络故障产生的原因往往是相当复杂的，特别是当故障是由多个网络组成部分共同引起的时候。在此情况下，一般先将网络修复，然后再分析网络故障的原因。分析故障原因对于防止类似故障的再次发生是相当重要的。网络故障管理包括故障检测、隔离和纠正三方面，应包括以下典型功能。

(1) 故障监测：主动探测或被动接收网络上的各种事件信息，并识别出与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

(2) 故障报警：接收故障监测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口、声音或音乐、电子邮件形式通知网络管理员。

（3）故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤和与故障相关的值班员日志，构造排错行动记录，将事件-故障-日志构成逻辑上相互关联的整体，以反映故障产生、变化、消除的整个过程的各个方面。

（4）排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错；根据已有的排错经验和管理员对故障状态的描述给出对排错行动的提示。

（5）检索/分析故障信息：浏览并且以关键字检索查询故障管理系统中所有的数据库记录，定期收集故障记录数据，在此基础上给出被管网络系统、被管线路设备的可靠性参数。

网络故障检测的依据是对网络组成部件状态的监测。不严重的简单故障通常被记录在错误日志中，并不作特别处理；而严重一些的故障则需要向网络管理系统“报警”。网络管理系统应根据有关信息对警报进行处理，排除故障。当故障比较复杂时，网络管理系统应能执行一些诊断测试来辨别故障原因。

1.4.2 计费管理

计费管理（accounting management）记录网络资源的使用，目的是控制和监测网络操作的费用和代价。它对一些公共商业网络尤为重要，它可以估算出用户使用网络资源可能需要的费用和代价，以及已经使用的资源。网络管理员还可规定用户可使用的最大费用，从而控制用户过多占用和使用网络资源，这也从另一方面提高了网络的效率。另外，当用户为了一个通信目的需要使用多个网络中的资源时，计费管理应可计算总计费用。计费管理通常包含以下内容。

（1）计费数据采集：计费数据采集是整个计费系统的基础，但计费数据采集往往受到采集设备硬件与软件的制约，而且也与进行计费的网络资源有关。

（2）数据管理与数据维护：计费管理人工交互性很强，虽然有很多数据维护工作由系统自动完成，但仍然需要人为管理，包括交纳费用的输入、联网单位信息维护，以及账单样式决定等。

（3）计费政策制定：由于计费政策经常灵活变化，因此实现用户自由制定输入计费政策尤其重要。这样需要一个制定计费政策的友好人机界面和完善的实现计费政策的数据模型。

（4）政策比较与决策支持：计费管理应该提供多套计费政策的数据比较，为政策制定提供决策依据。

（5）数据分析与费用计算：利用采集的网络资源使用数据、联网用户的详细信息以及计费政策计算网络用户的资源使用情况，并计算出应交纳的费用。

（6）数据查询：提供给每个网络用户关于自身使用网络资源情况的详细信息，网络用户根据这些信息可以计算、核对自己的收费情况。

1.4.3 配置管理

配置管理（configuration management）同样相当重要，它初始化网络并配置网络，以使其提供网络服务。配置管理是一组对辨别、定义、控制和监视组成一个通信网络的对象所必要的相关功能，目的是实现某个特定功能或使网络性能达到最优。配置管理通常包含以下内容。

(1) 配置信息的自动获取：在一个大型网络中，需要管理的设备是比较多的，如果每个设备的配置信息都完全依靠管理人员的手工输入，工作量是相当大的，而且还存在出错的可能性。对于不熟悉网络结构的人员来说，这项工作甚至无法完成。因此，一个先进的网络管理系统应该具有配置信息自动获取功能，即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。在网络设备的配置信息中，根据获取手段大致可以分为三类：第一类是网络管理协议标准的 MIB 中定义的配置信息；第二类是不在网络管理协议标准中有定义，但是对设备运行比较重要的配置信息；第三类是用于管理的一些辅助信息。

(2) 自动配置、自动备份及相关技术：配置信息自动获取功能相当于从网络设备中“读”信息，相应地，在网络管理应用中还有大量“写”信息的需求。同样根据设置手段对网络配置信息进行分类：第一类是可以通过网络管理协议标准中定义的方法进行设置的配置信息；第二类是可以通过自动登录到设备进行配置的信息；第三类是需要修改的管理性配置信息。

(3) 配置一致性检查：在一个大型网络中，由于网络设备众多，而且由于管理的原因，这些设备很可能不是由同一个管理人员进行配置的。实际上即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，对整个网络的配置情况进行一致性检查是必需的。在网络的配置中，对网络正常运行影响最大的主要是路由器端口配置和路由信息配置，因此，要进行一致性检查的也主要是这两类信息。

(4) 用户操作记录功能：配置系统的安全性是整个网络管理系统安全的核心，因此，必须对用户进行的每一配置操作进行记录。在配置管理中，需要对用户操作进行记录，并保存下来，管理人员可以随时查看特定用户在特定时间内进行的特定配置操作。

1.4.4 性能管理

性能管理(performance management)主要是监视和分析被管网络及其所提供的服务，收集分析有关被管网络当前状况的数据信息，维护和分析性能日志，以评估系统资源的运行状况及通信效率等系统性能。性能管理通常包括以下内容。

(1) 性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

(2) 阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阈值检查和告警，提供相应的阈值管理和溢出告警机制。

(3) 性能分析：对历史数据进行分析、统计和整理，计算性能指标，对性能状况作出判断，为网络规划提供参考。

(4) 性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

(5) 性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

1.4.5 安全管理

安全性一直是网络的薄弱环节之一，而用户对网络安全的要求又相当高，因此网络安全

管理(security management)非常重要。网络中主要有数据的私密性丢失、非授权访问等安全问题。相应地,网络安全管理应包括对授权机制、访问控制、加密的管理,另外还要维护和检查安全日志。

1. 网络安全管理机制

网络安全管理由以下机制来保证。

(1) 管理员身份认证:采用基于公开密钥的证书认证机制;为提高系统效率,对于信任域内的用户,可以使用简单口令认证。

(2) 管理信息加密与完整性:Web 浏览器和网络管理服务器之间采用安全套接字层(SSL)传输协议,对管理信息加密传输并保证其完整性;内部存储的机密信息,如登录口令等,也是经过加密的。

(3) 访问控制:网络用户按任务的不同分成若干用户组,不同的用户组有不同的权限范围,对用户的操作由访问控制检查,保证用户不能越权使用网络管理系统。

(4) 系统日志分析:记录用户所有的操作,使系统的操作和对网络对象的修改有据可查,同时也有助于故障的跟踪与恢复。

2. 网络对象的安全管理功能

网络对象的安全管理有以下功能。

(1) 网络资源的访问控制:通过管理路由器的访问控制表,完成防火墙的管理功能,即从网络层和传输层控制对网络资源的访问,保护网络内部的设备和应用服务,防止外来的攻击。

(2) 告警事件分析:接收网络对象所发出的告警事件,分析安全相关的信息,实时地向管理员告警,并提供历史安全事件的检索与分析机制,及时地发现正在进行的攻击或可疑的攻击迹象。

(3) 主机系统的安全漏洞检测:实时地监测主机系统的重要服务的状态,提供安全监测工具,以搜索系统可能存在的安全漏洞或安全隐患,并给出弥补的措施。

1.5 网络管理模型

在网络管理中,网络管理人员通过网络管理系统对网络资源的管理,普遍遵循的结构都是管理者-代理的管理模型,如图 1-1 所示。通常,一个网络管理系统从逻辑上由管理者(管理进程)、管理代理、管理信息库、管理协议 4 个要素组成。

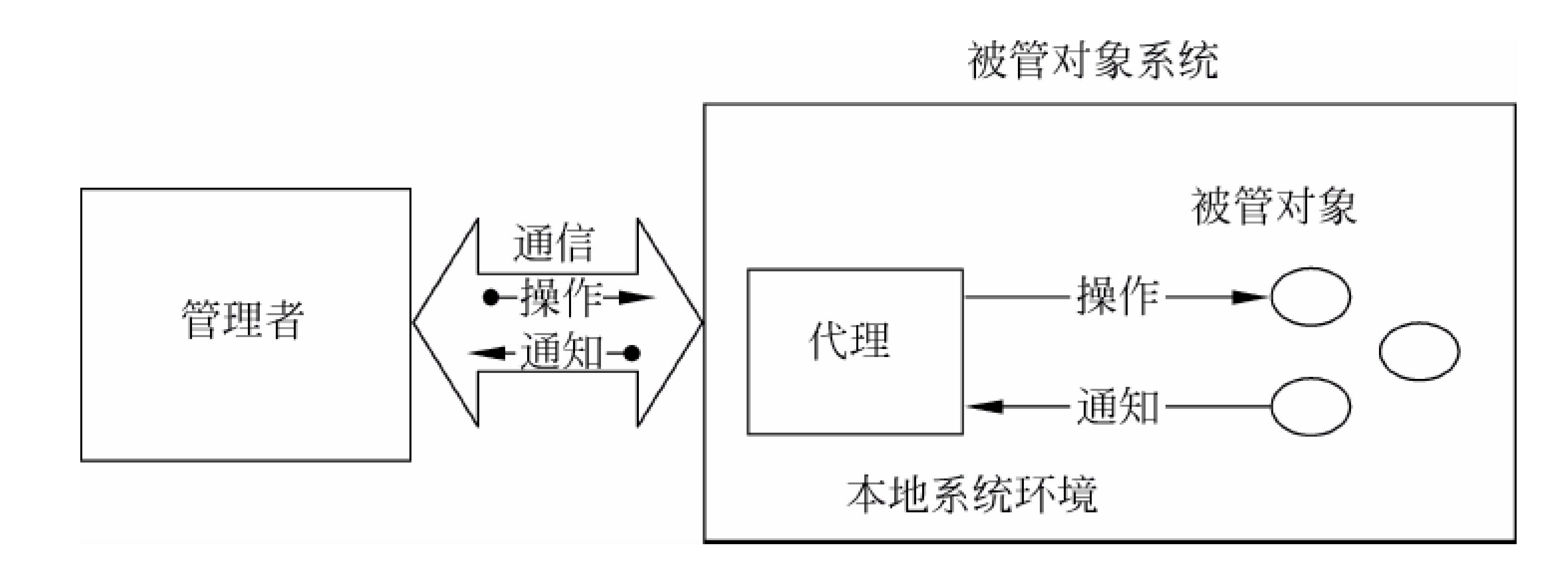


图 1-1 管理者-代理通信模型

(1) 管理者：网络管理者是一个控制台程序，是对网络设备和设施进行全面管理和控制的软件，一般位于网络系统的主干或主干位置，运行于网络管理中心工作站上，负责发出所有的控制指令与管理操作指令，实现对管理代理的操作与控制，并接收来自代理的信息，包括被管理的 TCP/IP 网络总体信息。其中的控制台程序提供 4 种功能，即：数据分析、故障恢复的管理应用程序；监视和控制网络的接口；把网络管理员的要求翻译成实际被管理网络元素；从网络中所有设备提取信息形成信息库。

(2) 管理代理：管理代理（简称代理）是应用进程中负责管理相关的被管理对象的部分，驻留于被管理网络设备上或被管网络应用处，实现搜索被管设备原始状态，它把来自管理者的命令或信息请示转换为自身设备特有的指令，完成管理者的指示，或反馈它所在的设备信息。另外，代理也可以把在自身系统中所发生的事件自动地通知给管理者。被管理的设备是需要被监控的网络部件或设施，包括工作站、服务器、网卡、交换机和路由器。

一个管理者可以和多个代理进行信息交互，同时一个代理也可以接受来自多个管理者的管理操作。一般的代理都是返回它本身设备的信息，在网络代理中还有另外一种代理——转换代理，它提供关于其他系统或其他设备的信息，使用转换代理，管理者可以管理多种类型的设备。

(3) 管理信息库（MIB）：MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库，由管理对象组成，各个代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。代理具有从 MIB 中读取各种变量值和在 MIB 中修改各种变量值两个基本功能。

(4) 管理协议：用于网络管理者和管理代理之间传递信息，并完成信息交换安全控制的通信规约称为网络管理协议。网络管理者通过网络管理协议从管理代理那里获取管理信息或向管理代理发送命令；管理代理也可以通过网络管理协议主动报告紧急信息。

1.6 网络管理标准

1.6.1 网络管理标准概述

为了能支持各种网络的互连及其管理，网络管理必须要遵从国际性的标准与协议。国际上有一些组织机构致力于研究、制定、开发网络管理的服务标准、协议和体系结构，其中最重要的有国际标准化组织（ISO）、国际电信联盟电信标准化部（ITU-T）和工程任务组（IETF）。

在这三个组织中，ISO 是第一个开发网络管理结构、制定网络管理标准的组织，早在 20 世纪 80 年代初期，ISO 就确定了网络管理体系结构作为其“开放系统互连（OSI）”工作的组成部分。至今，该组织已制定了大量的有关网络管理的标准，其内容统称为 OSI 系统管理。

从 1985 年开始，ITU（以前为 CCITT）致力于开发和制定电信网的网络管理标准，并且在 1988—1992 年的研究期间，引进了许多 OSI 管理思想，目前已经形成了较为完善的电信网络管理推荐标准，即 TMN 网络管理。由于前面一段的发展经历，实际上现在的 OSI 管理标准与 TMN 推荐标准可以互为补充。

20 世纪 80 年代后，Internet 发展迅猛，IETF 采用了基于 OSI 的 CMIP 协议作为

Internet 的管理协议，并对它作了修改，修改后的协议被称做 CMOT。但 CMOT 迟迟未能出台，IETF 决定把已有的 SGMP 进一步修改后，作为临时的解决方案。这个在 SGMP 基础上开发的解决方案就是著名的 SNMP。由于 SNMP 存在一些不足，IETF 已经提出了改进版本 SNMP v2，SNMP v3，在多个方面进行改进和强化。

从 20 世纪末开始，网络管理的概念已经逐渐超越了传统的在网络和网元管理层的五大管理功能，但还没有超出 TMN 定义的管理层次范围。电信管理论坛（TMF）提出的"新一代电信运营支撑系统"（NGOSS），涵盖了企业生产经营、网络运维、企业管理等各个层面，为企业的运营提供有效且完整的技术支持。NGOSS 中的电信运营业务框架 TOM 将一般的网管扩展到了 OSS 的全部范围，而其后的 eTOM 则进一步扩展到电信企业的 OSS/BSS。从目前规范涉及的主要内容来讲，eTOM 现有的内容主要相当于 TMN 中的商务管理层和业务管理层，而 SG4 的 TMN 中现有建议的主体是网络管理层和网元管理层。

从已有的标准和技术趋势来看，网络管理标准主要是在管理体系结构、管理信息模型和管理协议方面提出一些规范和建议。关于管理框架和体系结构的标准有 NGOSS（TMF）、OSS through Java（OSS/j），OSA/Parlay（ParlayConsortium，ETSI，3GPP），TMN（ITU-T）等。有关信息模型的标准有 TMF 的共享信息/数据模型（SID），核心事务实体（OSS/j），DMTF 的通用信息模型（CIM），OMG 的 MDA 等。关于管理协议方面的有 IETF 的 SNMP、COPS、LDAP，ITU-T 的 CMIP、IPDR，及另外一些用于通过 IP 传输数据的安全协议。

1.6.2 网络管理体系结构

定义网络管理系统的结构及系统成员间相互关系的一套规则称为网络管理体系结构。目前，典型网络管理体系结构有以下几种。

1. 基于 Internet/SNMP 的网络管理体系结构

SNMP 网络管理体系结构由管理者（管理进程）、代理和管理信息库三部分组成。管理者是管理指令的发出者，这些指令包括一些管理操作。管理者通过各设备的管理代理对网络内的各种设备、设施和资源实施监视和控制。代理负责管理指令的执行，并且以通知的形式向管理者报告被管对象发生的一些重要事件。

SNMP 是一个异步的请求/响应协议，SNMP 实体不需要在发出请求后等待响应到来。SNMP 中包括了 4 种基本的协议交互过程，即有 4 种操作：

- get 操作用来提取指定的网络管理信息。
- get-next 操作提供扫描 MIB 树和依次检索数据的方法。
- set 操作用来对管理信息进行控制。
- trap 操作用于通报重要事件的发生。

在这 4 个操作中，前三个请求是由管理者发给代理，需要代理发出响应给管理者，最后一个则是由代理发给管理者，但并不需要管理者响应。

SNMP 在计算机网络中应用非常广泛，已经成为事实上的计算机网络管理的标准。但是 SNMP 有许多缺点，是它自身难以克服的：

（1）SNMP 不适合真正大型网络管理，因为它是基于轮询机制的，这种方式有严重的性能问题。

（2）SNMP 不适合查询大量的数据。

（3）SNMP 的 trap 命令是无确认的，这样有可能导致不能确保非常严重的告警是否发送到管理者。

（4）安全管理较差。

（5）不支持如创建、删除动作等类型的操作，要完成这些操作，必须用 set 命令间接地触发。

（6）SNMP 的 MIB 模型不适合比较复杂的查询。

2. 基于 OSI/CMIP 的网络管理体系结构

在 OSI/CMIP 网络管理体系结构中，基本概念有系统管理应用进程（SMAP）、系统管理应用实体（SAME）、层管理实体和管理信息库（MIB）等。系统管理应用进程是执行系统管理功能的软件，它管理系统的各个方面并与其他系统的 SMAP 相互协调；系统管理应用实体负责与其他系统的对等 SAME 间交换管理信息，它包括如 SMAS、CMISE、ROSE 和 ACSE 等服务元素；层管理实体提供对 OSI 各层特定的管理功能；MIB 是系统中属于网络管理方面的信息的集合。

OSI 系统管理中用于定义和组织 MIB 的通用框架是管理信息模型（MIM），MIM 定义了如何表示与命名 MIB 中的资源。MIM 建立在面向对象的概念基础之上，对于每个要管理的资源，都抽象成管理对象（Managed Object，MO）。一个管理对象是从管理的角度采用面向对象方法对资源的一种抽象。通过封装的手段，管理对象屏蔽了与管理无关的资源信息，提供给管理系统一个用来交换管理信息的标准接口。

管理对象使用管理对象定义指南描述，MO 间的关系主要包括继承和包含关系。继承关系描述的是管理对象类之间的关系，它与面向对象方法中继承的概念是一致的。包含关系描述的是管理对象实例间的关系，实际上可以看做是现实世界中的包含关系。

OSI 系统管理中最基本的功能是在两个管理实体间通过协议交换管理信息。在 OSI 系统管理中，此项功能为 CMISE。CMISE 分为 CMIS 和 CMIP 两个部分：CMIS 描述提供给用户的服务；CMIP 描述完成 CMIS 服务的协议数据单元及其相关联的过程。CMIS 定义了提供给 OSI 系统管理的服务，这些服务由管理进程调用进行远程通信。CMIS 包括相关联服务、管理通知服务和管理操作服务，CMIS 共提供了 7 种服务原语。CMIP 定义了管理信息传输过程和 CMB 管理业务的语法，CMIP 是提供管理信息传输服务的应用层协议，它接受管理应用进程的 CMIS 服务原语，构造特定的应用层协议数据单元，通过会话层或其他协议层传送到对等的 CMIP 协议实体，再传送到用户进程。CMIP 支持 CMIS 提供的上述服务，它在 CMISE 间传递管理信息。

OSI/CMIP 网络管理体系结构是以更通用更全面的观点来组织一个网络的管理系统，它的开放性、着眼与网络未来发展的设计思想，使得它有很强的适应性，能够处理任何复杂系统的综合管理。然而正是 OSI 系统管理这种大而全的思想，导致其有如下缺点：

（1）OSI 系统管理违反了 OS 参考模型的基本思想。

（2）故障管理的问题。由于 OSI 系统管理用到了 OSI 各层的服务传送管理信息，使得 OSI 系统管理不能管理通信系统自己内部的故障。

（3）缺乏管理者特定的功能描述。OSI 系统管理标准仅仅定义了一个独立管理操作，但并没有定义这些操作的序列，以完成管理者要解决的特定问题。

(4) OSI 系统管理太复杂：CMIP 的功能极其灵活强大，使得 OSI 系统管理方法太复杂，从而 OSI 系统管理与实际的应用有距离，OSI 在实际应用中不成功。

(5) 缺乏相应的开发工具，这种开发工具可以使开发者不需了解 OSI 管理，而代理系统花费太高。

(6) OSI 系统管理不是纯面向对象的：OSI 系统管理虽然管理信息建模是面向对象的，但管理信息传送却不是面向对象的。

3. 基于 TMN 的网络管理体系结构

电信管理网(TMN)是一个逻辑上与电信网分离的网络，它通过标准的接口(包括通信协议和信息模型)与电信网传送/接收管理信息从而达到对电信网控制和操作的目的。TMN 的管理体系结构比较复杂，可以从 4 个方面分别进行描述：信息体系结构、功能体系结构、物理体系结构和逻辑分层体系结构。

(1) 信息体系结构

TMN 的信息体系结构基本上采用 OSI 系统管理概念和原则，如面向对象的建模方法、管理者与代理和 MIB 等。

(2) 功能体系结构

把 TMN 的功能划分为功能模块，每一功能模块又是由更小的功能单元来构成的，这是 TMN 的功能体系结构的基本原则。这一原则的目的是简化 TMN 的实现，把功能分布在不同的模块中，功能模块间利用数据通信功能来传递消息，并由功能参考点来分割，各模块可以独立实现，降低了 TMN 的复杂性，提高了软件的重用度。根据新版的 ITU-T M. 3011 的建议，TMN 的基本功能模块有 4 种：操作系统功能(OSF)、工作站功能(WSF)、Q 适配功能(QAF)和网元功能(NEF)，功能参考点分别为 q，f，x，g 和 m。

OSF 对管理信息进行处理以实现对电信网的监视、协调和控制。WSF 为用户提供接入到 TMN 的手段，其功能包括终端的安全接入和注册、识别、确认、输入输出、支持菜单、窗口和分页等。QAF 用来连接 TMN 实体与非 TMN 实体，提供 TMN 参考点与非 TMN 参考点之间的转换。NEF 表示被管理的功能，同时也提供管理时所需要的通信和支撑功能。

(3) 物理体系结构

根据需要，TMN 的功能结构可以灵活地组成不同的物理结构，物理结构由物理实体组成，物理实体之间为 TMN 的标准接口。TMN 的基本的物理实体包括操作系统(OS)、工作站(WS)、Q 适配器(QA)、网元(NE)和数据通信网(DCN)，它们之间的接口分别为 Q3 接口、F 接口和 X 接口。OS 主要完成 OSF 功能，同时也可完成 QAF 功能和 WSF 功能。WS 是完成 WSF 功能的系统，即完成 TMN 信息模型与人机界面表示形式之间转换的系统。QA 是连接非 TMN 网元和 TMN 操作系统之间的设备，完成 QAF 功能。NE 由电信设备和一些支撑设备组成，主要完成 NEF 功能，也可根据需要完成 TMN 中的其他功能，如 QAF、OSF 和 WSF 等。当功能模块在不同的物理实体中实现时，功能模块之间的功能参考点由物理实体之间的相应物理接口替代，如 Q3 接口在 q 参考点实现，F 接口在 f 参考点实现，X 接口在 x 参考点实现。若功能模块在一个物理实体中实现时，功能模块之间的功能参考点不转化为物理接口。

(4) 逻辑分层体系结构

电信网络的种类很多，电信网络的管理非常复杂，对各类电信设备的管理已经显示了其

复杂性，若对整个电信网，甚至只是对某个本地网做到综合管理都将是一项非常艰巨和非常复杂的任务。TMN 把管理功能需求分解为不同的层次，每层相对独立，都由各自的 OSF 完成特定的管理功能，层与层之间由 q 参考点分割。在 TMN 建设初期可以只完成低层的管理功能，以后逐步完善高层管理功能，最终实现管理的综合。TMN 的管理层次分为 5 层，从低到高依次为：网元层（NEL）、网元管理层（EML）、网络管理层（NML）、业务管理层（SML）和事务管理层（BML）。其中网元层属于被管理层，其他 4 层属于管理层。

TMN 从 20 世纪 80 年代中期提出后，已成为全球接受的管理电信公众网的框架。尽管 TMN 有技术上先进、强调公认的标准和接口等优点，但随着计算机和通信技术的不断发展，TMN 自身也暴露出许多问题，如目标太大、抽象化程度太高、MIB 的标准化进度太慢、OSI 协议栈效率不高等。下面具体分析 TMN 的不足：

(1) 在 TMN 中，接口是一个重要的内容，管理信息模型是接口中很重要的一部分。但到目前为止，TMN 只对网元层的管理信息模型进行了标准化，对网络管理层和业务管理层的管理信息模型，则只是才刚刚开始相关的标准化工作。

(2) TMN 管理分层问题。虽然 TMN 的逻辑分层体系结构对 TMN 功能进行分层，但到目前为止，TMN 重视网元层的功能和管理信息模型，网元层的重要性和作用已确定，但更高层和可被每一层接受的功能和管理信息模型则仍然在讨论中。

(3) TMN 的描述接口复杂，OSI 系统管理不稳定，TMN 的管理信息模型很难满足实际网管系统开发的需求。

(4) TMN 的管理信息模型是建立在 OSI 系统管理的基础之上的，它与 CMIP 协议是密切相关的，这种模型显然不适合计算机技术发展，如 CMIP 协议是面向事物的，基于数据流的，而分布式面向对象技术已成为当前计算机通信发展的趋势。GDMO/ASN. 1/CMIP 的信息模型不适用分布式面向对象技术。因此，需要建立与协议无关的管理信息模型。

(5) TMN 的信息体系结构缺乏对分布式管理的完全支持，虽然 TMN 提供管理者-代理模型，可以认为定义了一个分布式环境，但是，现存的信息体系结构在几个方面都对分布式透明有限制，例如，位置透明的通信方式是不可能的，充当管理者角色的应用进程必须知道代理进程的位置，为了完成一项任务，必须建立独立的通信实例。

(6) 在开发 TMN 应用程序时，缺乏可移植的、易用的、在 CMIP 之上的 API。虽然在一些无关平台上提供一些 API，但这些 API 要么复杂（XOM/XMP），要么是各平台特有的，不具备通用性，不具备可移植性。

1.7 本章小结

本章主要介绍了网络管理的基本概念、要素、目标、管理模型和体系结构等内容。

网络管理是指监督、控制网络资源的使用和网络的各种活动，使网络性能达到最佳的过程。即对网络的配置、运行状态和计费等所从事的全部操作和维护性活动。网络管理的目的在于提供对网络进行规划、设计、运行、分析、控制、评估和扩展的手段，从而合理地组织和利用网络资源，提供安全、可靠、高效和优质的服务。

网络管理系统的功能包括配置管理、性能管理、故障管理、计费管理和安全管理；网络管理模型主要是管理者-代理模型；网络管理体系结构有多种，目前应用最多的是 SNMP，

符合现代网络管理的其他新体系结构也正在研究和试验之中。

本章的重点是网络管理的基本概念、内容、目标和网络管理系统的五大功能。

习　题　1

一、选择题

1. 管理者和代理间的信息交换是通过(　　)进行的。

A. PDU　　B. Polling　　C. Heartbeat　　D. AC

2. 网络管理的要素包括(　　)。

A. 被管对象　　B. 管理方法　　C. 管理系统　　D. 管理模块

3. 下列选项中不是网络管理内容的是(　　)。

A. 运行　　B. 控制　　C. 计费　　D. 维护

4. 一个网络管理系统从逻辑上由管理者、管理代理、管理协议和(　　)组成。

A. 数据库　　B. 管理信息库　　C. 数据仓库　　D. 信息系统

5. 管理代理是应用进程中负责完成管理者的指示,并反馈其所在设备的信息,如果是非标准设备应该使用(　　)。

A. 设备代理　　B. 标准代理　　C. 代理插件　　D. 转换代理

6. SNMP 的四种操作中,(　　)是由代理发给管理者的,且不需要管理者响应。

A. trap　　B. get　　C. get-next　　D. set

二、简答题

1. 什么是网络管理?
2. 网络管理的目标是什么?
3. 网络管理系统的功能分别是什么?
4. 网络管理体系结构有哪些?
5. 轮询和心跳机制有什么区别?
6. 请说明网络管理模型的原理。

第 2 章 管理信息库

管理信息库(Management Information Base,MIB)是一个概念上的数据库,定义了一个网络中所有可能的被管理对象的集合的数据结构,指明了网络元素所维持的变量(即能够被管理进程查询和设置的信息)。本章将介绍 MIB 的相关知识。

2.1 管理信息库概述

MIB 是网络管理数据的标准,在这个标准里规定了网络代理设备必须保存的数据项目、数据类型,以及允许在每个数据项目中的操作。通过对这些数据项目的存取访问,就可以得到被管对象的所有统计内容。再通过对多个统计内容的综合分析即可实现基本的网络管理。

MIB 由 IETF 定义,规范了可访问的网络设备及其属性,每个网络设备由对象识别符(Object Identifier,OID)唯一指定。MIB 是 SNMP 的基础,每个被管资源由对象来表示,MIB 是这些对象的有结构的集合。MIB 本质上是一个树型的数据结构,网络中每个被管对象(工作站、服务器、路由器、网桥等)都拥有一个反映其状态的 MIB,网络管理实体可以通过提取 MIB 中的对象值监测系统中的资源,也可以通过修改这些对象值来控制资源。

MIB 的定义与具体的网络管理协议无关,这对于厂商和用户都有利。厂商可以在产品中包含 SNMP 代理软件,并保证在定义新的 MIB 项目后该软件仍遵守标准。用户可以使用同一网络管理客户软件来管理具有不同版本的 MIB 的多个网络设备。当然,一个没有新的 MIB 项目的网络设备不能提供这些项目的信息。

2.2 管理信息结构

2.2.1 管理信息结构(SMI)的定义

1. 管理信息结构的概念

管理信息结构(Structure of Management Information,SMI)是简单网络管理协议(SNMP)的一部分,其指定了在 SNMP MIB 中用于定义管理目标的规则。SMI 被划分为三个部分:模块定义、对象定义和陷阱定义。

MIB 的总体框架、数据类型的表示方法和命名方法是由 SMI 定义和说明的,是 MIB 中对象定义和编码的基础。SMI 为定义和构造 MIB 提供了一个通用的框架,同时也规定了可

以在 MIB 中使用的数据类型，说明了资源在 MIB 中怎样表示和命名。SMI 的基本指导思想是追求 MIB 的简单性和可扩充性，因此，MIB 只能存储简单的数据类型：标量和标量的二维矩阵。

SMI 避开复杂的数据类型是为了降低实现的难度和提高互操作性。但在 MIB 中不可避免地包含厂家建立的数据类型，如果对这样的数据类型的定义没有严格的限制，互操作性也会受到影响。为了提供一个标准的方法来表示管理信息，SMI 必须：

- 提供一个标准的技术定义 MIB 的具体结构。
- 提供一个标准的技术定义各个对象，包括句法和对象值。
- 提供一个标准的技术对对象值进行编码。

2. SMI 的定义

MIB 中存在的数据叫做对象，每个对象都有一个类型和一个值。类型是对被管对象种类的定义，因此类型的定义是一个句法描述。对象的实例是某类对象的一个具体实现，具有一个确定的值。

MIB 中的对象用抽象语法表示（Abstract Syntax Notation Number One，ASN.1）来描述。ASN.1 是一种形式语言，它提供了统一的网络数据表示，用于定义应用数据的抽象语法和应用层协议数据单元结构。用 ASN.1 定义的抽象数据在传送过程中按照基本编码规则（Basic Encoding Rule，BER）变换成比特串，这就构成了在网络上传送的数据包。

ASN.1 中包含了一些预定义的通用类型，也规定了通过现有类型定义新类型的语法。定义被管对象的一个可选方法是定义一个被称为 Object 的新类型，这样，MIB 中所有的对象都将是这种类型。这个方法在技术上是可行的，但会产生定义不便于应用的问题，因为在实践中可能需要定义多种数据类型。另外，MIB 支持二维表格或矩阵的定义，因此，一个通用的对象类型必须包含参数来对应所有这些可能性和选择性。

另一个更有吸引力的方法，并且也是被 SNMP 所实际采用的方法是利用宏（macro）对在被管对象定义中相互关联的类型进行集合定义。一个宏的定义给出相关类型集合的句法，而宏的实例定义一个特定的类型，因此定义被分为以下等级。

- 宏：定义合法的宏实例，即说明相关集合类型的句法。
- 宏实例：通过为宏定义提供实际参数生成实例，即说明一个特定的类型。
- 宏实例值：用一个特定的值来表示一个特定的实体。

图 2-1 是 OBJECT-TYPE 宏的定义（RFC 1212）。

下面介绍 OBJECT-TYPE 宏中的主要项目。

- SYNTAX：对象类的抽象句法，该句法必须从 SMI 的对象句法类型中确定一种类型。
- ACCESS：定义通过 SNMP 或其他协议访问对象实例的方法。Access 子句定义该对象类型支持的最低等级，可选的等级有：read-only、read-write、write-only 和 not-accessible。
- STATUS：指出该对象在实现上的要求。要求可以是：mandatory（必须）、optional（可选）、deprecated（恳求——必须实现的对象，但很可能在新版 MIB 中被删除）和 obsolete（废除——不再需要被管系统实现的对象）。
- DescrPart：对象类型语义的文本描述，该子句是可选的。

```
OBJECT-TYPE MACRO ::=
BEGIN
    TYPE NOTATION ::="SYNTAX" type(ObjectSyntax)
                    "ACCESS" Access
                    "STATUS" Status
                    DescrPart
                    ReferPart
                    IndexPart
                    DefValPart
    VALUE NOTATION ::= value (VALUE ObjectName)
    Access ::= "read-only"| "read-write"| "write-only"| "not-accessible"
    Status ::= "mandatory"| "optional"| "obsolete"| "deprecated"
    DescrPart ::="DESCRIPTION" value (description DisplayString)| empty
    ReferPart ::="REFERENCE" value (reference DisplayString)| empty
    IndexPart ::="INDEX" "{" IndexTypes "}"| empty
    IndexTypes ::=IndexType | IndexTypes "," IndexType
    IndexType ::=value (indexobject ObjectName)| type (indextype)
    DefValPart ::="DEFVAL" "{" value (defvalue ObjectSyntax) "}"| empty
END
```

图 2-1　被管对象宏

- ReferPart：对定义在其他 MIB 模块中的某个对象的文本型交叉引用。该子句是可选的。
- IndexPart：用于定义表。该子句只是在对象类型对应表中的“行”时才出现。
- DefValPart：定义一个默认值，用于建立对象实例，该子句是可选的。
- VALUE NOTATION：指出通过 SNMP 访问该对象时使用的名字。

由于应用 OBJECT-TYPE 宏的 MIB 的完整的定义包含在 MIB 的冗长的文档中，因此，人们并不常使用它们。比较常用的是更简捷的方法——基于树型结构和对象特性的表格表示的方法。

2.2.2　MIB 的结构

1. MIB 树型结构

SNMP 中的所有的被管对象都被排列在一个树型结构之中，如图 2-2 所示。处于叶子位置上的对象是实际的被管对象，每个实际的被管对象表示某些被管资源、活动或相关信息。树型结构本身定义一个将对象组织到逻辑上相关的集合之中的方法，这种结构的意义如下。

（1）表示管理和控制的关系

上层的中间节点是某些组织机构的名字，表示这些机构分别负责对其下面子树的管理工作。有些中间节点虽然不是组织机构名，但已经委托某个组织机构代管。

（2）提供了结构化的信息组织技术

图中下层的节点代表的子树是与每个网络资源或网络协议相关的信息集合，沿着树层次访问相关信息非常灵活和方便。

（3）提供了对象命名机制

树中的每个节点都有一个分层的编号，叶子节点代表实际的管理对象，从树根到树叶的编号串联起来，用圆点隔开，就形成了管理对象的标识。

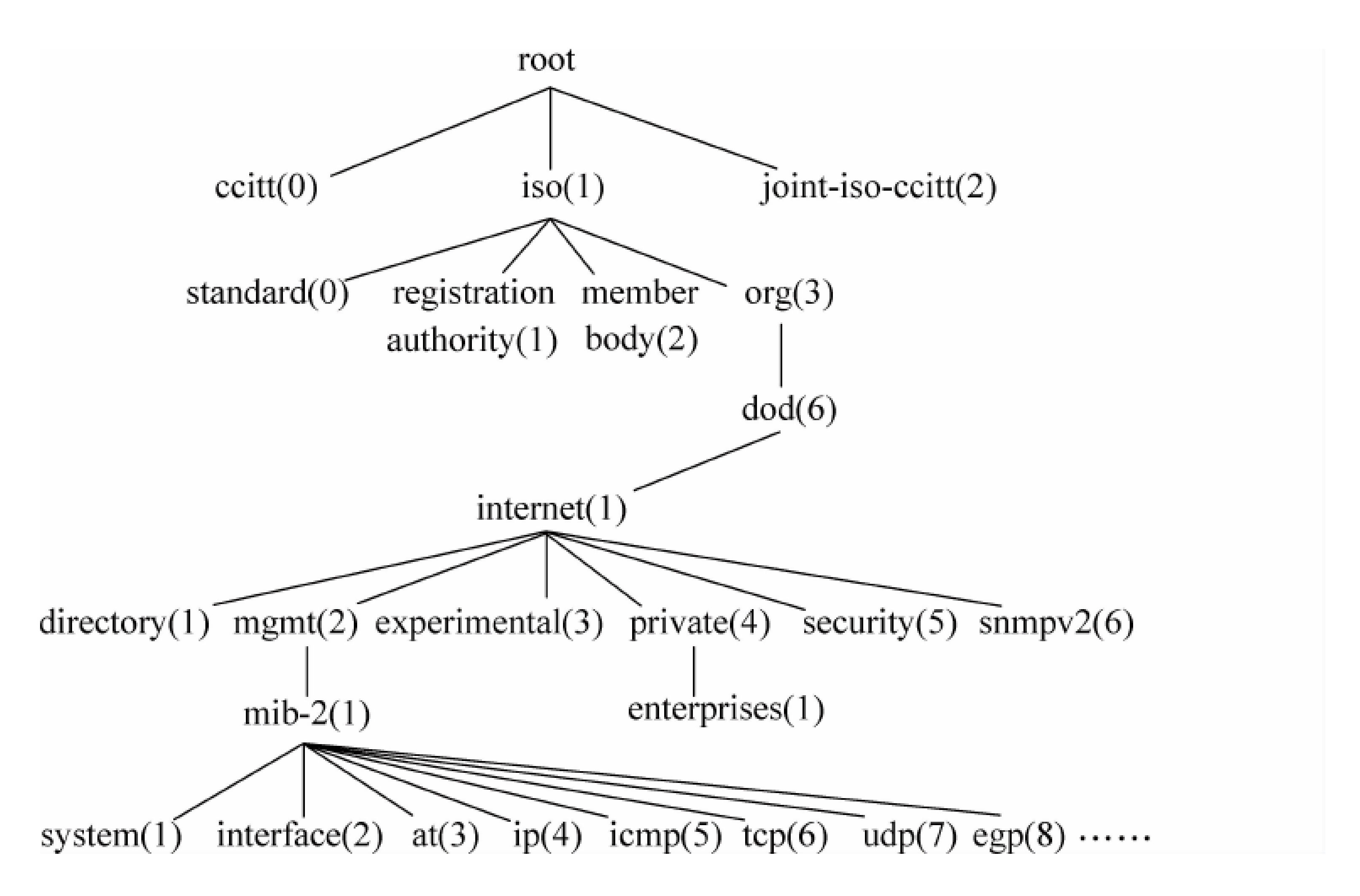


图 2-2　对象标识符树型结构

使用这个树状分层结构，MIB 浏览器能够以一种方便而且简捷的方式访问整个 MIB 数据库。MIB 浏览器是这样一种工具，它可以遍历整棵 MIB 结构树，通常以图形显示的形式来表示各个分枝和树叶对象。可以通过其数字标识符来查找 MIB 中的数据对象，这个数字标识符号从 MIB 结构树的根部开始，直到各个叶子节点为止。这种访问方式和文件系统的组织方式一致。

2. 对象标识

MIB 中的每个对象类型都被赋予一个对象标识符，以此来命名对象。另外，由于对象标识符的值是层次结构的，因此命名方法本身也能用于确认对象类型的结构。

对象标识符是能够唯一标识某个对象类的符号，它的值由一个整数序列构成，被定义的对象的集合具有树型结构，树根是引用 ASN.1 标准的对象。从对象标识符树的树根开始，每个对象标识符成分的值指定树中的一个弧，从树根开始，第一级有 3 个节点：iso、ccitt、joint-iso-ccitt。在 iso 节点下面有一个为"其他组织"使用的子树 org，其中有一个美国国防部的子树（dod），SNMP 在 dod 之下设置一个子树用于 Internet 的管理，如下所示为 internet OID：

```
internet OBJECT IDENTIFIER :: = { iso (1) org (3) dod (6) 1}
```

因此，internet 节点的对象标识符的值是 1.3.6.1，这个值作为 internet 子树的下级节点标识符的前缀。SMI 在 SNMP v1 中的 internet 节点之下定义了如下文所述的 4 个节点：

- directory(1)为与 OSI 的 directory 相关的为将来的应用保留的节点。
- mgmt(2)用于在 IAB 批准的文档中定义的对象。
- experimental(3)用于标识在 Internet 实验中应用的对象。
- private(4)用于标识单方面定义的对象。

在 SNMP v2 中增加了 Security(5)和 Snmpv2(6)两个节点。

mgmt 子树包含 IAB 已经批准的管理信息库的定义，现在已经开发了两个版本的 MIB，mib-1 和它的扩充版 mib-2。二者子树中的对象标识符是相同的，因为在任何配置中，

只有一个 MIB。最初的节点 MIB 将其所管理的信息分为 8 个类别，现在的 mib-2 所包含的信息类别已超过 40 个。

private 子树目前只定义了一个子节点 enterprises{1.3.6.1.4.1}，用于厂商加强对自己设备的管理，与用户及其他厂商共享信息。在 enterprises 子树下面，每个注册了 enterprises 对象标识符的厂商有一个分支，其所属节点数已超过 3000。例如 IBM 为{1.3.6.1.4.1.2}，Cisco 为{1.3.6.1.4.1.9}，Novell 为{1.3.6.1.4.1.23}等。世界上任何一个公司、学校，只要用电子邮件发往 iana-mib@isi.edu 进行申请，即可获得一个节点名。这样各厂家就可以定义自己的产品的被管理对象名，使它能用 SNMP 进行管理。

internet 节点之下分为 4 个子树的做法为 MIB 的进化提供了很好的基础，通过对新对象的实验，厂商能够在其被接受为 mgmt 的标准之前有效地获得大量的实际知识。因此这样的 MIB 既是对管理符合标准的对象直接有效的，对适应技术和产品的变化也是灵活的，这一点也反映了 TCP/IP 协议在成为标准之前进行大量的实验性的使用和调测的特性。

2.2.3 MIB 中的数据类型

SNMP MIB 中的每个对象都有一个形式化的方法定义，说明对象的数据类型、取值范围以及与 MIB 中的其他对象的关系。各个对象以及 MIB 的整体结构都由 ASN.1 描述法定义，为了保持简单，只利用了 ASN.1 的元素和特征的一个有限的子集。

1. UNIVERSAL 类型

ASN.1 的 UNIVERSAL 类由独立于应用的通用数据类型组成，其中只有以下数据类型被允许用于定义 MIB 对象：

- integer (UNIVERSAL 2)
- octetstring (UNIVERSAL 4)
- null (UNIVERSAL 5)
- object identifier (UNIVERSAL 6)
- sequence，sequence of (UNIVERSAL 16)

前 3 个是构成其他对象类型的基本类型。object identifier 是唯一标识对象的符号，由一个 integer 序列组成，序列中的 integer 被称为子标识符。对象标识符的 integer 序列从左到右，定义了对象在 MIB 树型结构中的位置。sequence 和 sequence of 用于构成表。

2. APPLICATION-WIDE 类型

ASN.1 的 APPLICATION 类由与特定的应用相关的数据类型组成。每个应用，包括 SNMP，负责定义自己的 APPLICATION 数据类型，在 SNMP 中已经定义了以下数据类型：

- networkaddress：该类型用 CHOICE 结构定义，允许从多个协议簇的地址格式中进行选择，目前只定义了 IPAddress 一种地址格式。
- ipaddress：IP 格式的 32 位地址。
- counter：只能做增值不能做减值运算的非负整数，最大值被设为 $2^{32}-1$，当达到最大值时，再次从 0 开始增加。
- gauge：既可做增值也可做减值运算的非负整数，最大值被设为 $2^{32}-1$，当达到最大值时被锁定，直至被复位(reset)。

- timeticks：从某一参照时间开始以百分之一秒为单位计算经历的时间的非负整数。当 MIB 中定义的某个对象类用到这个数据类型时，参照时间在该对象类的定义中指出。
- opaque：该数据类型提供一个传递任意数据的能力。数据在传递时被作为 Octet string 编码。被传递的数据本身可以是由 ASN.1 或其他句法定义的任意的格式。

2.2.4 标量对象和表对象

SNMP 的变量可分为两种，一种是标量，另一种是用二维数组组织的表变量。

SMI 只支持一种数据结构化方法，即标量值条目的二维表。表是对象的有序集合，包含若干行。有些数据的组织用表格来表达比较方便，多个对象的组合能够完整地描述一条信息。表的定义用到 ASN.1 的 sequence 和 sequence of 两个类型和 OBJECT-TYPE 宏中的 IndexPart。

表定义方法可以通过实例进行说明。考虑对象类型 tcpConnTable，这个对象包含由相应的被管实体维护的 TCP connections 的信息。对于每个这样的 connection，以下信息在表中存储：

- state：TCP connection 的状态。
- local address：该 connection 的本端的 IP 地址。
- local port：该 connection 的本端的 TCP 端口。
- remote address：该 connection 的另一端的 IP 地址。
- remote port：该 connection 的另一端的 TCP 端口。

需要注意的是，tcpConnTable 是存放在某个被管系统维护的 MIB 之中的，因此，tcpConnTable 中的一个条目对应被管系统中的一个 connection 的状态信息。TCP connection 的状态信息有 22 个项目，按照 tcpConnTable 的定义，只有上述 5 个项目对网络管理者来说是可见的。这也体现了 SNMP 强调保持网络管理简单性的特点，即在被管对象中，只包含相对应的被管实体的有限的和有用的信息。图 2-3 给出了 tcpConnTable 的定义(RFC1213)。

在图 2-3 中，可以看到 sequence 和 sequence of 在定义表时的应用。整个表由一个 SEQUENCE OF TcpConnEntry 构成，ASN.1 的结构 SEQUENCE OF 由一个或多个相同的元素构成，在本例中(在所有的 SNMP SMI 的情况下)每个元素是表中的一行。

每一行由一个指定了 5 个标量元素的 SEQUENCE 构成，ASN.1 的结构 SEQUENCE 由固定数目的元素组成，元素的类型可以是多种。尽管 ASN.1 允许这些元素是可选的，但 SMI 限制这个结构只能使用“mandatory”元素。在本例中，每一行所包含的元素的类型是 INTEGER、IPAddress、INTEGER、IpAddress 和 INTEGER。

tcpConnEntry 定义中的 INDEX 成分确定哪个对象值将被用于区分表中的各行。在 TCP 中，一个 socket (IP 地址，TCP 端口)可以支持多个 connection，而任意一对 sockets 之间同时只能有一个 connection。因此为了明确地区分各行，每行中的后 4 个元素是必要的，也是充分的。

SNMP 表的常用操作是取值(取整个表的对象实例的值、取行的值、取列的值)、修改值、添加行、删除行和遍历整个表。其实这些操作都是基于 get、set、getNext、getBulk、response 这几个基本操作实现的。

```
tcpConnTable OBJECT-TYPE
              SYNTAX   SEQUENCE OF TcpConnEntry
              ACCESS   not-accessible
              STATUS   mandatory
              DESCRIPTION
                 "A table containing TCP connection-specific information."
              ::= { tcp 13 }
          tcpConnEntry OBJECT-TYPE
              SYNTAX   TcpConnEntry
              ACCESS   not-accessible
              STATUS   mandatory
              DESCRIPTION
                   "Information about a particular current TCP connection.  An object of this
                    type is transient,in that it ceases to exist when (or soon after) the
                    connection makes the transition to the CLOSED state."
              INDEX { tcpConnLocalAddress,
                      tcpConnLocalPort,
                      tcpConnRemAddress,
                      tcpConnRemPort }
              ::= { tcpConnTable 1 }
          tcpConnEntry ::=SEQUENCE {tcpConnState INTEGER,
                                    tcpConnLocalAddress IpAddress,
                                    tcpConnLocalPort  INTEGER (0..65535),
                                    tcpConnRemAddress IpAddress,
                                    tcpConnRemPort INTEGER (0..65535)}
          tcpConnState OBJECT-TYPE
              SYNTAX   INTEGER  {closed(1),listen(2),synSent(3),synReceived(4),
                established(5),finWait1(6),finWait2(7),closeWait(8),lastAck(9),closing(10),
                timeWait(11),deleteTCB(12)}
              ACCESS   read-write
              STATUS   mandatory
              DESCRIPTION
                       "The state of this TCP connection.…"
              ::= { tcpConnEntry 1 }
```

图 2-3　TCPConn Table 的定义

2.2.5　对象实例的标识

MIB 中的每个对象都有一个由其在树型结构的 MIB 中所处的位置所定义的唯一的对象标识符。但是，应该注意到，MIB 树型结构给出的对象标识符在一些情况下只是对象类型的标识符，不能唯一地标识对象的实例。例如表格的对象标识符不能标识表格中各个条目。由于对 MIB 的访问是对对象实例的访问，因此各个对象实例都必须有唯一标识的方法。

1. 表与列对象

表中的对象被称为列对象。列对象标识符不能独自标识对象实例，因为表中的每一行都有列对象的一个实例。为了实现这类对象实例的唯一标识，SNMP 实际定义了词典顺序访问和随机访问两种技术。词典顺序访问技术是利用词典编排顺序实现的；而随机访问技术是利用索引对象值实现的。

(1) 随机访问技术

一个表格是由零到多个行(条目)构成的，每一行都包含一组相同的标量对象类型(或称列对象)。每个列对象都有一个唯一的标识符。但由于列对象可能有多个实例，因此列对象

标识符并不能唯一标识它的各个实例。然而,在定义表格时,一般包含一个特殊的列对象INDEX,即索引对象,它的每个实例都具有不同的值,可以用来标识表中的各行。因此,SNMP采用将索引对象值连接在列对象标识符之后的方法来标识列对象的实例。

例如interfaces组中的ifTable,如图2-5(c)所示。表中有一个索引对象ifIndex,它的值是一个1到ifNumber之间的整数,对应每个接口,ifIndex有一个唯一的值。现在假设要获取系统中第2个接口的接口类型ifType,ifType的对象标识符是1.3.6.1.2.1.2.2.1.3,而第2个接口的ifIndex值是2,因此对应第2个接口的ifType的实例的标识符便为1.3.6.1.2.1.2.2.1.3.2。即将这个ifIndex的值作为实例标识符的最后一个子标识符加到ifType对象标识符之后。

(2) 词典顺序访问技术

对象标识符是反映该对象在MIB中的树型结构的一个整数序列。在MIB的树型结构中,跟踪从root开始到某个特定对象的路径,便可以得到该对象的对象标识符。即,可以通过遍历MIB中的对象标识符树来生成对象实例的词典顺序。

因为管理者对代理提供MIB视图的构成不一定完全清楚,因此它需要一种不必提供对象名称就能访问对象的方法。在这种情况下,对象及其实例的排序就是非常重要的,利用这个排序,管理者可以有效地遍历一个MIB的结构。因为管理者只要提供树型结构的任意一点上的一个对象实例的标识符,就可以顺序地对其后继的对象实例进行访问。例如,要检索一个表项,管理者可以连续发出get操作,按词典顺序得到预定的对象实例。

表2-1为一个简化的IP路由表,这个路由表的对象及其实例按分层树排列如图2-4所示,表2-2给出了对应的词典顺序。

表2-1　简化的路由表

ipRouteDest	ipRouteMetric1	ipRouteNextHop
9.1.2.3	3	99.0.0.3
10.0.0.51	5	89.1.1.42
10.0.0.99	5	89.1.1.42

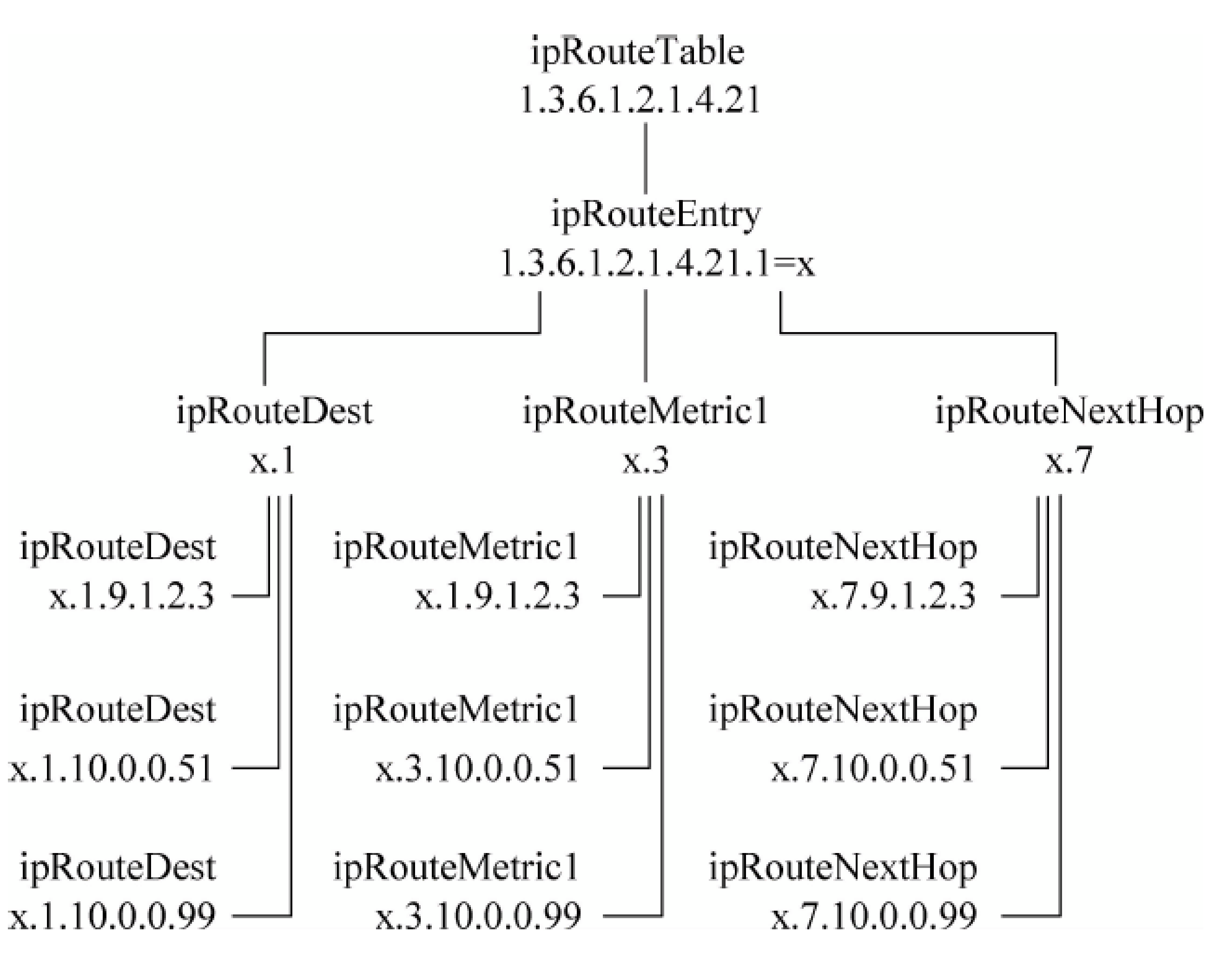


图2-4　IP路由表对象及其实例的子树

表 2-2　IP 路由表对象及其实例的词典顺序

对　　象	对象标识符	下一个对象实例
ipRouteTable	1.3.6.1.2.1.4.21	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteEntry	1.3.6.1.2.1.4.21.1	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteDest	1.3.6.1.2.1.4.21.1.1	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteDest.9.1.2.3	1.3.6.1.2.1.4.21.1.1.9.1.2.3	1.3.6.1.2.1.4.21.1.1.10.0.0.51
ipRouteDest.10.0.0.51	1.3.6.1.2.1.4.21.1.1.10.0.0.51	1.3.6.1.2.1.4.21.1.1.10.0.0.99
ipRouteDest.10.0.0.99	1.3.6.1.2.1.4.21.1.1.10.0.0.99	1.3.6.1.2.1.4.21.1.3
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3	1.3.6.1.2.1.4.21.1.3
ipRouteMetric1.9.1.2.3	1.3.6.1.2.1.4.21.1.3.9.1.2.3	1.3.6.1.2.1.4.21.1.3.10.0.0.51
ipRouteMetric10.0.0.51	1.3.6.1.2.1.4.21.1.3.10.0.0.51	1.3.6.1.2.1.4.21.1.3.10.0.0.99
ipRouteMetric.10.0.0.99	1.3.6.1.2.1.4.21.1.3.10.0.0.99	1.3.6.1.2.1.4.21.1.7.9.1.2.3
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7	1.3.6.1.2.1.4.21.1.7.9.1.2.3
ipRouteNextHop1.9.1.2.3	1.3.6.1.2.1.4.21.1.7.9.1.2.3	1.3.6.1.2.1.4.21.1.7.10.0.0.51
ipRouteNextHop10.0.0.51	1.3.6.1.2.1.4.21.1.7.10.0.0.51	1.3.6.1.2.1.4.21.1.7.10.0.0.99
ipRouteNextHop.10.0.0.99	1.3.6.1.2.1.4.21.1.7.10.0.0.99	1.3.6.1.2.1.4.21.1.1.x

2. 表与行对象

对于表格和行对象，没有定义它们的实例标识符。这是因为表格和行不是叶子对象，因而不能由 SNMP 访问。在这些对象的 MIB 定义中，它们的 ACCESS 特性被设为 not-accessible。

3. 标量对象

在标量对象的场合，用对象类型标识符便能唯一标识它的实例，因为每个标量对象类型只有一个对象实例。但是，为了与表格对象实例标识符的约定保持一致，也为了区分对象的类型和对象实例，SNMP 规定标量对象实例的标识符由其 OID 后加“0”来标识，如 sysName 变量的 OID 是“.iso.org.dod.internet.mgmt.mib-2.system.sysName.0”。

2.3　MIB-2 功能组

在 TCP/IP 网络管理的建议标准中，提出了多个相互独立的 MIB，其中包含为 Internet 的网络管理而开发的 MIB-2。MIB-2 是在 MIB-1 的基础之上开发的，是 MIB-2 的一个超集。MIB-2 组被分为 11 个功能组，共 171 个对象。但 MIB-2 只包括那些被认为是必要的对象，不包括任选的对象。对象的分组方便了管理实体的实现，一般来说，制造商如果认为某个功能组是有用的，则必须实现该组的所有对象。

2.3.1　system 组

system 组提供有关被管系统的总体信息，如图 2-5(a)所示。表 2-3 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-3　system 组中的对象

对象名称	语　　法	访问权限	功能描述
sysDescr	DisplayString (SIZE(0 … 255))	RO	对实体的描述，如硬件、操作系统等
sysObjectID	OBJECT IDENTIFIER	RO	实体中包含的网络管理子系统的厂商标识
sysUpTime	TimeTicks	RO	系统的网络管理部分本次启动以来的时间
sysContact	DisplayString (SIZE(0 … 255))	RW	该被管节点负责人的标识和联系信息
sysName	DisplayString (SIZE(0 … 255))	RW	该被管节点被赋予的名称
sysLocation	DisplayString (SIZE(0 … 255))	RW	该节点的物理地点
sysServices	INERGER (0 … 127)	RO	指出该节点所提供的服务的集合，7 个 bit 对应 7 层服务

2.3.2　interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息，如图 2-5(c)所示。这个功能组是必须实现的。

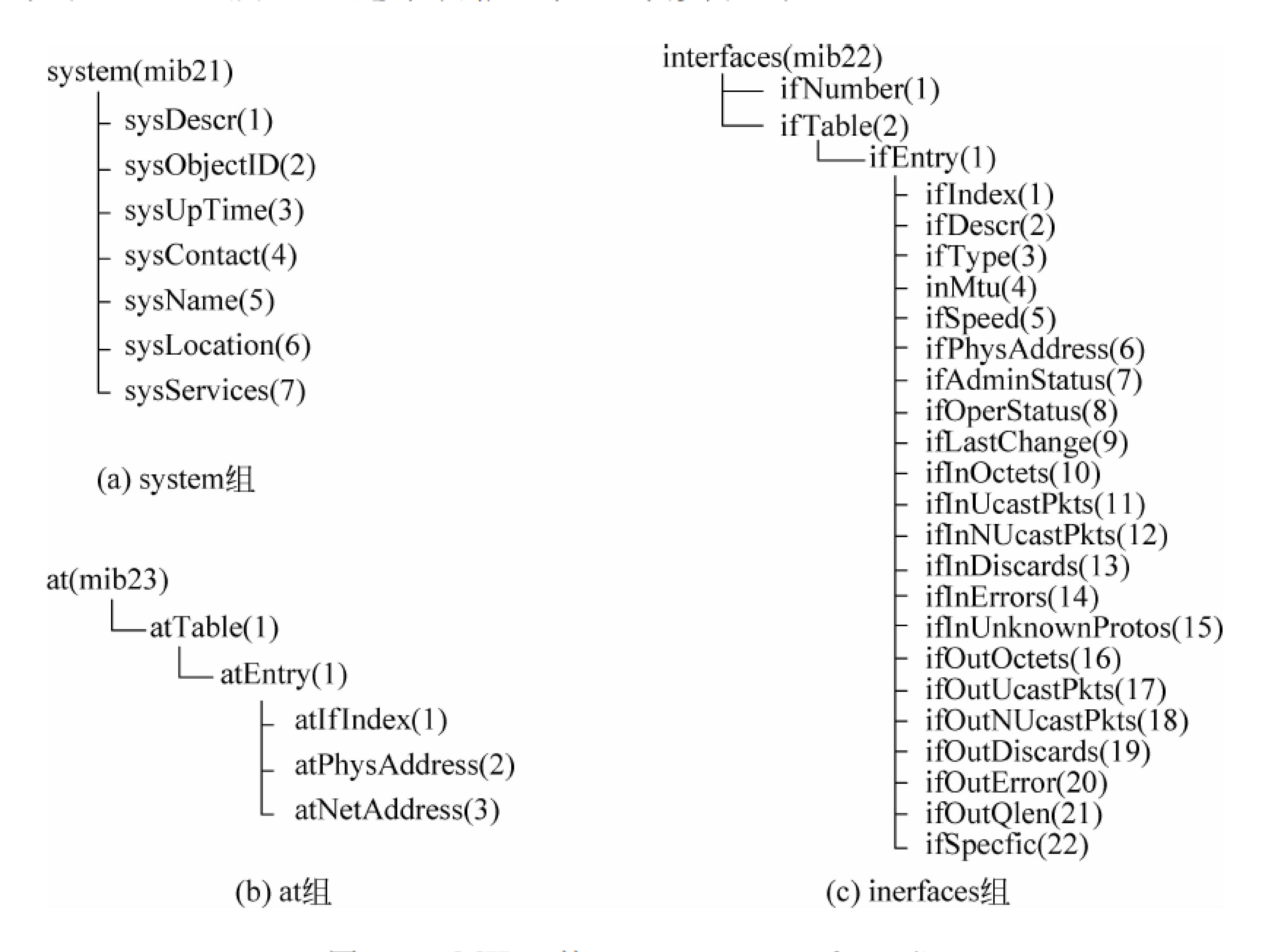


图 2-5　MIB-2 的 system、at、interfaces 组

interfaces 接口组中的对象可用于故障管理和性能管理，例如，可以通过检查进出接口的字节数或队列长度来检测网络拥塞；可以通过接口状态获知工作情况；还可以统计出输入输出的错误率等。表 2-4 为该组中各个对象的名称、语法、访问权限和功能描述。

表 2-4　interfaces 组中的对象

对象名称	语　法	访问权限	功能描述
ifNumber	INTEGER	RO	网络接口的数目
ifTable	SEQUENCE OF ifEntry	NA	接口条目清单
ifEntry	SEQUENCE	NA	包含子网及其以下层对象的接口条目
ifIndex	INTEGER	RO	对应各个接口的唯一值
ifDescr	DisplayString (SIZE(0 … 255))	RO	有关接口的信息，包括厂商、产品名称、硬件接口版本
ifType	INTEGER	RO	接口类型，根据物理或链路层协议区分
ifMtu	INERGER	RO	接口可接收或发送的最大协议数据单元的尺寸
ifSpeed	Gauge	RO	接口当前数据速率的估计值
ifPhysAddress	PhysAddress	RO	网络层之下协议层的接口地址
ifAdminStatus	INTEGER	RW	期望的接口状态(up(1),down(2),testing(3))
ifOperStatus	INTEGER	RO	当前的操作接口状态(up(1),down(2),testing(3))
ifLastChange	TimeTicks	RO	接口进入当前操作状态的时间
ifInOctets	Counter	RO	接口收到的 8 元组的总数
ifInUcastPkts	Counter	RO	递交到高层协议的子网单播的分组数
ifInNUcastPkts	Counter	RO	递交到高层协议的非单播的分组数
ifInDiscards	Counter	RO	被丢弃的进站分组数
ifInErrors	Counter	RO	有错的进站分组数
ifInUnkownProtos	Counter	RO	由于协议未知而被丢弃的分组数
ifOutOctets	Counter	RO	接口发送的 8 元组的总数
ifOutUcastPkts	Counter	RO	发送到子网单播地址的分组总数
ifOutNUcastPkts	Counter	RO	发送到非子网单播地址的分组总数
ifOutDiscards	Counter	RO	被丢弃的出站分组数
ifOutErrors	Counter	RO	不能被发送的有错的分组数
ifOutQLen	Gauge	RO	输出分组队列长度
ifSpecific	OBJECT IDENTIFIER	RO	参考 MIB 对实现接口的媒体的定义

2.3.3　at 组

at(address translation)组由一个表构成，如图 2-5(b)所示。表中的每一行对应系统中的一个物理接口，提供网络地址向物理地址的映射。一般情况下，网络地址是指系统在该接口上的 IP 地址，而物理地址决定于实际采用的子网情况。例如，如果接口对应的是 LAN，则物理地址是接口的 MAC 地址，如果对应 X. 25 分组交换网，则物理地址可能是一个 X. 121 地址。表 2-5 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-5　address translation 组中的对象

对象名称	语　法	访问权限	功能描述
atTable	SEQUENCE OF AtEntry	NA	包含网络地址对物理地址的映射
atEntry	SEQUENCE	NA	包含一个网络地址、物理地址对
atIfIndex	INTEGER	RW	表格条目的索引
atPhysAddress	PhysAddress	RW	依赖媒体的物理地址
atNetAddress	NetworkAddress	RW	对应物理地址的网络地址

实际上，address translation 组包含在 MIB-2 中只是为了与 MIB-1 兼容，MIB-2 的地址转换信息在各个网络协议组中提供。

2.3.4 ip 组

ip 组包含有关节点上 IP 实现和操作的信息，如有关 IP 层流量的一些计数器等。ip 组的对象如图 2-6(a)所示，这些对象分为 4 大类，包括有关性能和故障监控的标量对象，以及 3 个表对象：ipAddrTable、ipRouteTalbe 和 ipNetToMediaTable。

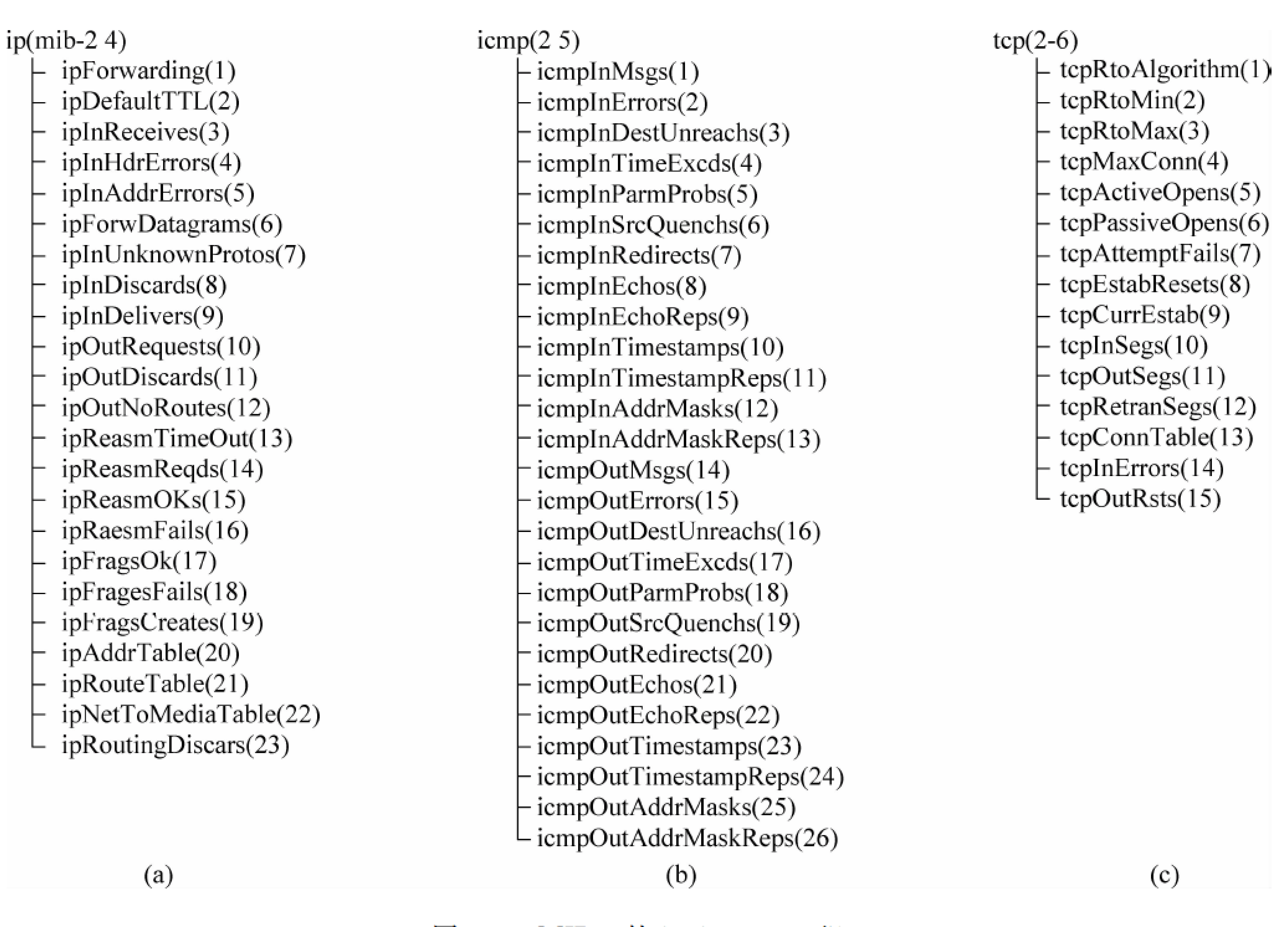


图 2-6 MIB-2 的 ip、icmp、tcp 组

ipAddrTable 包含分配给该实体的 IP 地址的信息，每个地址被唯一地分配给一个物理地址。

ipRouteTable 包含用于互联网路由选择的信息，该路由表中的信息是从一些协议的路由表中抽取而来的。实体当前所知的每条路由都有一个条目，表格由 ipRouteDest 索引。ipRouteTable 中的信息可用于配置的监测，并且由于表中的对象是 read-write 的，因此也可被用于路由控制。

ipNetToMediaTable 是一个提供 IP 地址和物理地址之间对应关系的地址转换表。除了增加一个指示映射类型的对象 ipNetToMediaType 之外，表中所包含的信息与 address translation 组相同。

此外，ip 组中还包含一些用于性能和故障监测的标量对象。表 2-6 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-6 ip 组中的对象

对象名称	语法	访问权限	功能描述
ipForwarding	INTEGER	RW	是否作为 IP 网关(1/0)
ipDefaultTTL	INTEGER	RW	插入到该实体生成的数据报的 IP 头中 Time-To-Live 字段中的默认值
ipInReceives	Counter	RO	接口收到的输入数据报的总数
ipInHdrErrors	Counter	RO	由于 IP 头错被丢弃的输入数据报总数
ipInAddrErrors	Counter	RO	由于 IP 地址错被丢弃的输入数据报总数
ipForwDatagrams	Counter	RO	转发的输入数据报数
ipInUnknownProtos	Counter	RO	由于协议未知被丢弃的输入数据报数
ipInDiscards	Counter	RO	无适当理由而被丢弃的输入数据报数
ipInDelivers	Counter	RO	成功地递交给 IP 用户协议的输入数据报数
ipOutRequests	Counter	RO	本地 IP 用户协议要求传输的 IP 数据报总数
ipOutDiscards	Counter	RO	无适当理由而被丢弃的输出数据报数
ipOutNoRoutes	Counter	RO	由于未找到路由而被丢弃的 IP 数据报数
ipReasmTimeOut	INTEGER	RO	重组接收到的碎片可等待的最大秒数
ipReasmReqds	Counter	RO	接收到的需要重组的 IP 碎片数
ipReasmOKs	Counter	RO	成功重组的 IP 数据报数
ipRaesmFails	Counter	RO	由 IP 重组算法检测到的重组失败的数目
ipFragsOk	Counter	RO	成功拆分的 IP 数据报数
ipFragsFails	Counter	RO	不能成功拆分而被丢弃的 IP 数据报数
ipFragsCreates	Counter	RO	本实体产生的 IP 数据报碎片数
ipAddrTable	SEQUENCE OF IpAddrEntry	NA	本实体的 IP 地址信息
ipRouteTable	SEQUENCE OF IpRouteEntry	NA	IP 路由表
ipNetToMediaTable	SEQUENCE OF IpNetToMedia Entry	NA	用于将 IP 映射到物理地址的地址转换表
IpRouting Discards	Counter	RO	被丢弃的路由选择条目

2.3.5 icmp 组

icmp(Internet Control Message Protocol)是 TCP/IP 协议簇中的一部分,所有实现 IP 协议的系统都提供 icmp。icmp 提供从路由器或其他主机向主机传递消息的手段,它的基本作用是反馈通信环境中存在的问题。

icmp 组包含有关一个节点的 icmp 的实现和操作的信息,它所包含的对象如图 2-6(b)所示,表 2-7 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-7 icmp 组中的对象

对象名称	语法	访问权限	功能描述
icmpInMsgs	Counter	RO	收到的 ICMP 消息的总数
icmpInErrors	Counter	RO	收到的有错的 ICMP 的消息数
icmpInDestUnreachs	Counter	RO	收到的目的地不可到达的消息数

续表

对象名称	语　法	访问权限	功能描述
icmpInTimeExcds	Counter	RO	收到的超时的消息数
icmpInParmProbs	Counter	RO	收到的有参数问题的消息数
icmpInSrcQuenchs	Counter	RO	收到的源有问题的消息数
icmpInRedirects	Counter	RO	收到的重定向的消息数
icmpInEchos	Counter	RO	收到的要求 echo 的消息数
icmpInEchoReps	Counter	RO	收到的应答 echo 的消息数
icmpInTimestamps	Counter	RO	收到的要求 Timestamp 的消息数
icmpInTimestampReps	Counter	RO	收到的应答 Timestamp 的消息数
icmpInAddrMasks	Counter	RO	收到的要求 Address Mask 的消息数
icmpInAddrMaskReps	Counter	RO	收到的应答 Address Mask 的消息数
icmpOutMsgs	Counter	RO	发出的 ICMP 消息的总数
icmpOutErrors	Counter	RO	发出的有错的 ICMP 的消息数
icmpOutDestUnreachs	Counter	RO	发出的目的地不可到达的消息数
icmpOutTimeExcds	Counter	RO	发出的超时的消息数
icmpOutParmProbs	Counter	RO	发出的有参数问题的消息数
icmpOutSrcQuenchs	Counter	RO	发出的源有问题的消息数
icmpOutRedirects	Counter	RO	发出的重定向的消息数
icmpOutEchos	Counter	RO	发出的要求 echo 的消息数
icmpOutEchoReps	Counter	RO	发出的应答 echo 的消息数
icmpOutTimestamps	Counter	RO	发出的要求 Timestamp 的消息数
icmpOutTimestampReps	Counter	RO	发出的应答 Timestamp 的消息数
icmpOutAddrMasks	Counter	RO	发出的要求 Address Mask 的消息数
icmpOutAddrMaskReps	Counter	RO	发出的应答 Address Mask 的消息数

2.3.6　tcp 组

tcp 组包含有关一个节点的 TCP 的实现和操作的信息，它所包含的对象如图 2-6(c)所示。表 2-8 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-8　tcp 组中的对象

对象名称	语　法	访问权限	功能描述
tcpRtoAlgorithm	INTEGER	RO	重传时间
tcpRtoMin	INTEGER	RO	重传时间的最小值
tcpRtoMax	INTEGER	RO	重传时间的最大值
tcpMaxConn	INTEGER	RO	实体支持的 TCP 连接数的上限
tcpActiveOpens	Counter	RO	实体已经支持的主动打开的数量
tcpPassiveOpens	Counter	RO	实体已经支持的被动打开的数量
tcpAttemptFails	Counter	RO	已经发生的试连失败的次数
tcpEstabResets	Counter	RO	已经发生的复位的次数
tcpCurrEstab	Gauge	RO	当前状态为 established 的 TCP 连接数
tcpInSegs	Counter	RO	收到的 segments 总数
tcpOutSegs	Counter	RO	发出的 segments 总数

续表

对象名称	语　法	访问权限	功能描述
tcpRetranSegs	Counter	RO	重传的 segments 总数
tcpConnTable	SEQUENCE OF TcpConnTntry	NA	包含 TCP 各个连接的信息
tcpInErrors	Counter	RO	收到的有错的 segments 的总数
tcpOutRsts	Counter	RO	发出的含有 RST 标志的 segments 数

2.3.7 udp 组

udp 组包含有关一个节点的 UDP 的实现和操作的信息，所包含的对象如图 2-7(a)所示。除了有关发送和接收的数据报的信息之外，这个组中还包含一个 udpTable 表，该表中包含 UDP 端点的管理信息。所谓 UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 表中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。

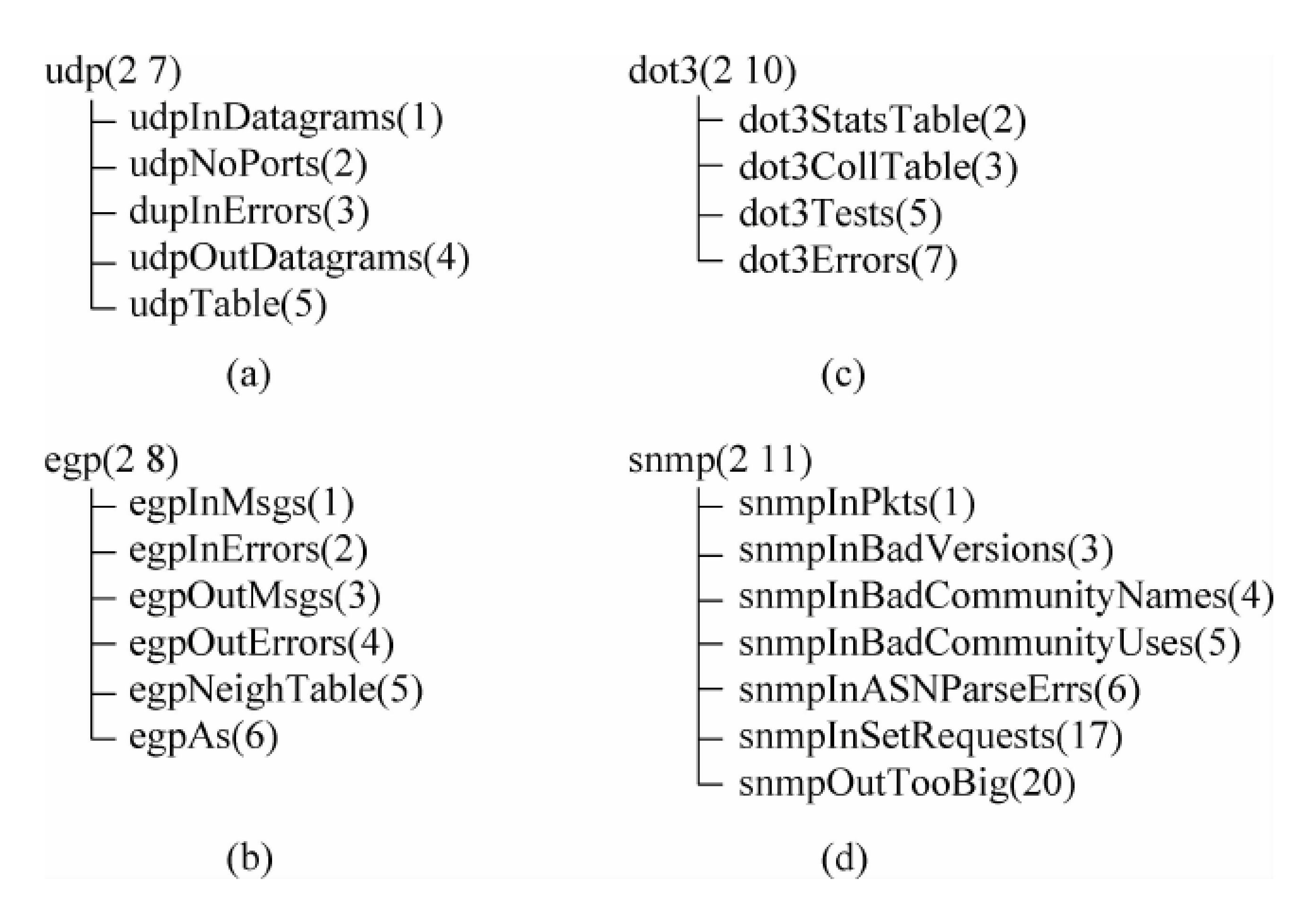


图 2-7　MIB-2 的 udp、egp、dot3、snmp 组

表 2-9 列出了 udp 组中各个对象的名称、语法、访问权限和功能描述。

表 2-9　udp 组中的对象

对象名称	语　法	访问权限	功能描述
udpInDatagrams	Counter	RO	递交该 UDP 用户的数据报的总数
udpNoPorts	Counter	RO	收到的目的端口上没有应用的数据报总数
udpInErrors	Counter	RO	收到的无法递交的数据报数
udpOutDatagrams	Counter	RO	该实体发出的 UDP 数据报总数
udpTable	SEQUENCE OF UdpEntry	NA	包含 UDP 的用户信息

2.3.8 egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)的实现和操作的信息，所包含的对象如图 2-7(b)所示。除了有关发送和接收的 EGP 消息的信息之外，这个组中还包含一个 egpNeighTable 表，该表中包含有关相邻网关的信息。表 2-10 列出了该组中各个

对象的名称、语法、访问权限和功能描述。

表 2-10　egp 组中的对象

对象名称	语　　法	访问权限	功能描述
egpInMsgs	Counter	RO	收到的无错的 EGP 消息数
egpInErrors	Counter	RO	收到的有错的 EGP 消息数
egpOutMsgs	Counter	RO	本地产生的 EGP 消息总数
egpOutErrors	Counter	RO	由于资源限制没有发出的本地产生的 EGP 消息数
egpNeighTable	SEQUENCE OF EgpNeighEntry	NA	相邻网关的 EGP 表(表内的对象略)
egpAs	INTEGER	RO	本 EGP 实体的自治系统数

2.3.9　dot3 组

dot3(transmission)组包含的对象提供关于系统上每个已定义接口的下层数据链路介质的细节。事实上,dot3 组并不能真正算是一个组,更像是 MIB-2 分支层次上的一个节点,该组的主要目的是用特定接口的 MIB 形式提供特定接口信息。interfaces 组在一个给定系统上提供应用于所有接口的一般信息;特定接口 MIB 在 dot3 下包含的信息是关于某个特定数据链路协议的。

图 2-7(c)展示了 dot3 组包括的四个表:dot3StatsTable、dot3CollTable、dot3Tests 和 dot3Errors。

dot3StatsTable 表记录代理和物理网络介质之间获得的流量统计数据。需要用一个表来代替一组特定计数器是因为工作站、服务器和其他网络设备可能包含多于一个的网络接口。因此,对系统上定义的每一个接口有一个表项。该表由 dot3StatsIndex 对象 x 索引。表 2-11 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-11　dot3 组中的对象

对象名称	语　　法	访问权限	功能描述
dot3StatsTable	Counter	RO	包含从代理软件和网络介质之间接口上获得的网络流量统计数据
dot3CollTable	Counter	RO	包含代理和网络介质之间在网络上观察到冲突活动的记录
dot3Tests	Counter	RO	测试接口
dot3Errors	Counter	RO	报告错误时使用

2.3.10　snmp 组

snmp 组包含 SNMP 操作和执行的相关信息,该组中的一些对象是与 SNMP 管理或代理功能相关的。所以,每个 SNMP 的实现可能使用该表中的某些对象,那些代理不支持的对象将包含零值。

图 2-7(d)展示了 snmp 表的树型视图,已经作废的节点并没有列出,这是因为当 SNMP v2 规范发表后,许多对象被取消了。然而,由于许多代理继续支持 SNMP v1,所以这些对

象仍在使用,早先的 snmp 组对象将继续使用一段较长的时间。表 2-12 列出了该组中各个对象的名称、语法、访问权限和功能描述。

表 2-12 snmp 组中的对象

对象名称	语法	访问权限	功能描述
snmpInPkts	Counter	RO	传递给该代理的 SNMP 消息的数量
snmpInBadVersions	Counter	RO	传递给该代理,但该代理不支持的 SNMP 消息的数量
snmpInBadCommunityNames	Counter	RO	传递给该代理的包含未知区名的 SNMP 消息的数量
snmpInBadCommunityUses	Counter	RO	传递给该代理的某种 SNMP 消息的数量,这种 SNMP 消息包含一个 SNMP 操作,但该操作根据提供的区名而不允许执行
snmpInASNParseErrs	Counter	RO	对输入的 SNMP 消息解码时,发生 BER 和 ASN 错误的数量
snmpInSetRequests	Counter	RO	由该代理接受并处理的 SNMP set-requests 的数量
snmpOutTooBig	Counter	RO	由该代理产生的 SNMP PDU 发生 tooBig 错误的数量

2.3.11 cmot 组

前面介绍了 MIB-2 中除了 cmot 组之外的 10 个组,cmot 组因为开发陷于停顿状态,所以暂不讨论。实际上 MIB 本身是在不断的扩充之中,目前的对象有近 20 个。

2.4 本章小结

本章首先介绍了管理信息库(MIB)的概念;然后介绍了管理信息结构(SMI)的概念、MIB 的结构、MIB 的数据类型、标量对象和表结构的表示方法等内容;最后对 MIB-2 功能组进行了介绍。

SMI 定义了一些通用规则,包括命名对象,定义对象类型,以及如何把对象和值进行编码。MIB 在需要被管理的实体中创建了命名对象、它们的值以及它们彼此之间关系的集合。MIB 如同程序设计语言中的定义变量,包括变量类型和名称;SMI 则如同程序设计语言中定义的编码规则、语法、变量的结构、数据类型等。

本章重点是掌握 MIB、SMI 的相关概念;理解对象标识、实例表示的规则和方法;了解 MIB-2 组中相关对象的功能。

习 题 2

一、选择题

1. SMI 包括三个部分,它们分别是(　　)。

A. 陷阱定义　　B. 对象定义　　C. 表定义　　D. 模块定义

2. mgmt 节点的对象标识符是(　　)。

A. 1.3.6.1　　B. 1.3.6.1.1　　C. 1.3.6.1.2　　D. 1.3.6.1.1.3

3. 为了实现表对象实例的唯一标识,SNMP 定义了(　　)访问技术。

A. 顺序　　B. 链式　　C. 随机　　D. 树型

4. 标量对象类型只有一个对象实例。为了与表格对象实例标识符的约定保持一致，也为了区分对象的类型和对象实例，SNMP 规定标量对象实例的标识符由其 OID 后加(　　)来标识。

A. 0　　B. 1　　C. 2　　D. 特殊字符

5. (　　)组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息，这个功能组是必须实现的。

A. ip　　B. system

C. address translation　　D. interfaces

二、简答题

1. 什么是 MIB?
2. 什么是 SMI?
3. SNMP 中管理对象是如何组织的?
4. MIB-2 中的管理对象分哪几个组?
5. 对象标识符是由什么组成的? 网络中的设备是如何表示的?
6. 什么是标量对象和表? 它们的实例是如何标识的?

第3章 网络管理协议

网络管理系统中最重要的部分就是网络管理协议，它定义了网络管理者和被管代理间的通信方法。目前主流的网络管理协议有简单网络管理协议(SNMP)、公共管理信息服务/公共管理信息协议(CMIS/CMIP)等。

3.1 简单网络管理协议

3.1.1 SNMP的发展

在TCP/IP的早期开发中，网络管理问题并未得到足够的重视，直到20世纪70年代，还一直没有网络管理协议，只有互联网络控制信息协议(ICMP)可以作为网络管理的工具。但是到了20世纪80年代后期，当互联网络的发展呈指数增长时，人们才意识到需要开发功能更强并易于普通网络管理人员学习和使用的标准协议。

1987年11月发布的SGMP，成为提供专用网络管理工具的起点。SGMP提供了一个直接监控网关的方法，随着对通用网络管理工具需求的增长，出现了3个有影响的方法：

- 高层实体管理系统(HEMS)：主机监控协议(HMP)的一般化。
- 简单网络管理协议(SNMP)：SGMP的升级版。
- TCP/IP上的CMIP(CMOT)：最大限度地与OSI标准的CMIP、服务以及数据库结构保持一致。

1988年，IAB确定了将SNMP作为近期解决方案进一步开发，因为SNMP开发速度快，并能为网络管理经验库的开发提供一些基本的工具，因此可用来满足眼前的需要；而把CMOT作为远期解决方案的策略。当时普遍认为TCP/IP不久将会过渡到OSI，因而不应在TCP/IP的应用层协议和服务上花费太多的精力。

为了强化这一策略，IAB要求SNMP和CMOT使用相同的被管对象数据库，两个协议都以相同的格式使用相同的监控变量。因此，两个协议有一个公共的SMI和一个MIB。但是，人们很快发现这两个协议在对象级兼容是不现实的，因此IAB最终放松了公共SMI/MIB的条件，并允许SNMP独立于CMOT发展。从对OSI的兼容性的束缚中解脱后，SNMP取得了迅速的发展，很快被众多的厂商设备所支持。

但是，当SNMP被用于大型或复杂网络时，它在安全性和功能方面的不足就变得明显了。为了弥补这些不足，1992年7月发表了3个增强SNMP安全性的文件作为建议标准。增强版与原来的SNMP是不兼容的，它需要改变外部报文句柄及一些报文处理过程。但实际定义协议操作并包含SNMP报文的协议数据单元(PDU)保持不变，并且没有增加新的

PDU,目的是尽量实现向 SNMP 的安全版本的平滑过渡。同样是在 1992 年 7 月,提出一个称为 SMP 的 SNMP 新版本。SMP 在功能和安全性两方面提高了 SNMP,所有的报文头和安全功能都与提议的安全性增强标准相似。最终 SMP 被接受为定义 SNMP v2 的基础,1993 年安全版 SNMP v2 发布。

经过几年试用以后,IETF 决定对 SNMP v2 进行修订,1996 年 SNMP v2 的安全特性被取消了,报文格式也重新采用 SNMP v1 的基于"共同体(community)"概念的格式。删除安全特性是 SNMP v2 发展过程中最大的失败。

1999 年 4 月 IETF SNMP v3 工作组提出了 RFC2571～RFC2576,形成了 SNMP v3 的建议。SNMP v3 提出了 SNMP 管理框架的一个统一的体系结构,在这个体系结构中,采用 User-based 安全模型和 View-based 访问控制模型提供 SNMP 网络管理的安全性。安全机制是 SNMP v3 的最具特色的内容。

3.1.2 SNMP 的体系结构

SNMP 体系结构的基本框架分以下 4 方面说明。

1. 网络管理体系结构

SNMP 的网络管理模型包括以下关键元素:管理者、代理、管理信息库、网络管理协议。管理者一般是一个分立的设备,也可以利用共享系统实现。管理者被作为网络管理员与网络管理系统的接口,它的基本构成如下:

- 一组具有分析数据、发现故障等功能的管理程序。
- 一个用于网络管理员监控网络的接口。
- 将网络管理员的要求转变为对远程网络元素的实际监控能力。
- 一个从所有被管网络实体的 MIB 中抽取信息的数据库。

网络管理系统中另一个重要元素是代理——装备了 SNMP 的平台,如主机、网桥、路由器及集线器均可作为代理工作。代理对来自管理者的信息请求和动作请求进行应答,并随机地为管理者报告一些重要的意外事件。

与 CMIP 体系相同,网络资源也被抽象为对象进行管理,但 SNMP 中的对象是表示被管资源某一方面的数据变量。对象被标准化为跨系统的类,对象的集合被组织为 MIB。MIB 作为设在代理处的管理者访问点的集合,管理者通过读取/设置 MIB 中对象的值来进行网络监控。管理者可以在代理处产生动作,也可以通过修改变量值改变代理处的配置。

管理者和代理之间通过网络管理协议通信,SNMP 通信协议主要包括以下能力:

- get——管理者读取代理处对象的值。
- set——管理者设置代理处对象的值。
- trap——代理向管理者通报重要事件。

在标准中,没有特别指出管理者的数量及管理者与代理的比例。一般地,应至少要有两个系统能够完成管理者功能,以提供冗余度,防止故障。另一个实际问题是一个管理者能带动多少代理,只要 SNMP 保持它的简单性,这个数量可以高达几百。

2. 网络管理协议体系结构

SNMP 为应用层协议,是 TCP/IP 协议簇的一部分,它通过 UDP 来操作。在分立的管

理者中,管理进程对位于管理者中心 MIB 的访问进行控制,并提供网络管理员接口,管理进程通过 SNMP 完成网络管理。SNMP 在 UDP、IP 及有关的特殊网络协议之上实现。

每个代理也必须实现 SNMP、UDP 和 IP。另外,有一个解释 SNMP 的报文和控制代理 MIB 的代理进程。

图 3-1 描述了 SNMP 的协议环境,从管理者发出 3 类与管理应用有关的 SNMP 的报文 GetRequest、GetNextRequest、SetRequest。3 类报文都由代理用 GetResponse 报文应答,该报文被上交给管理应用。另外,代理可以发出 Trap 报文,向管理者报告有关 MIB 及管理资源的事件。

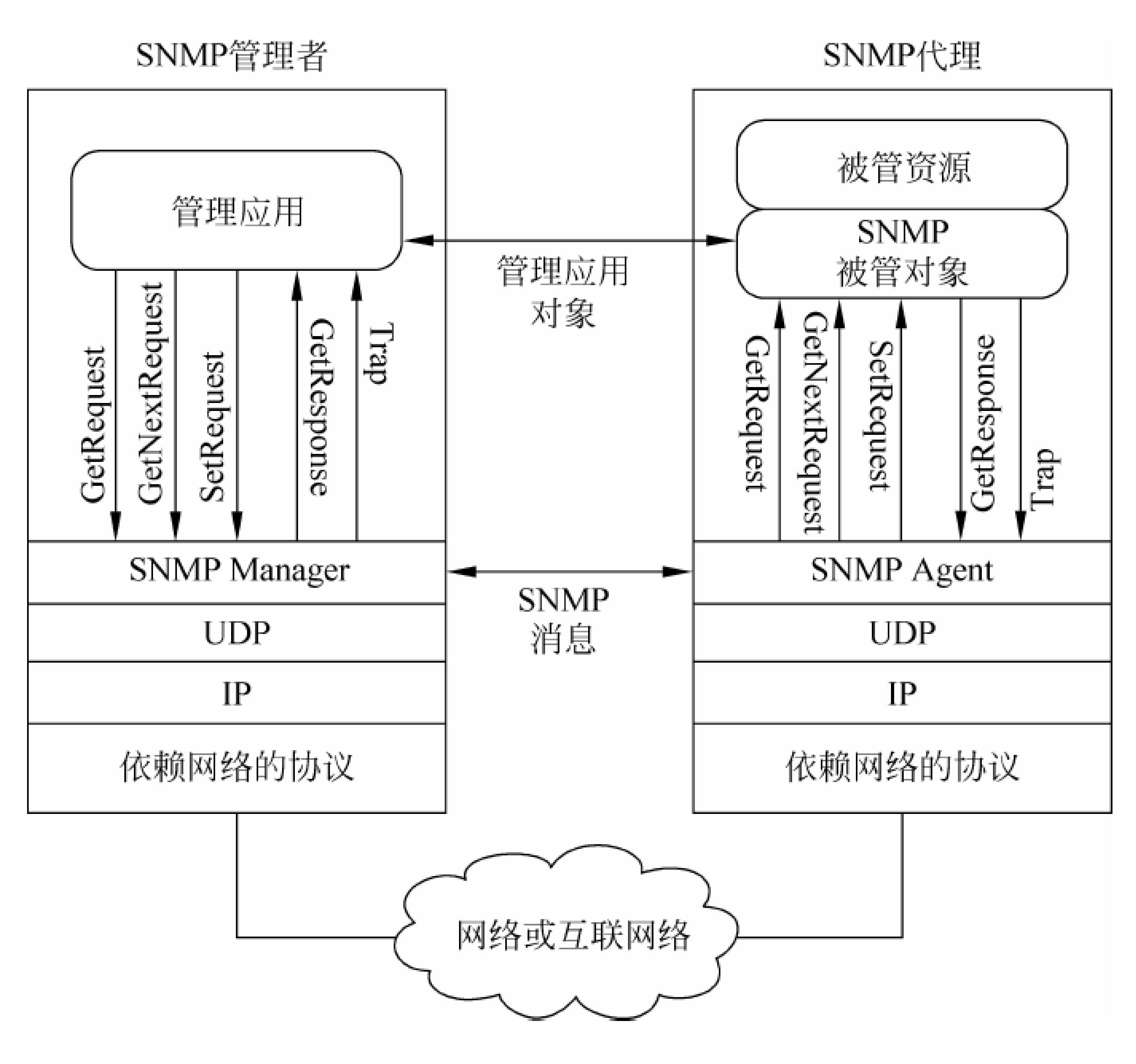


图 3-1　SNMP 的协议环境

由于 SNMP 依赖 UDP,而 UDP 是无连接型协议,所以 SNMP 也是无连接型协议。在管理者和代理之间没有在线的连接需要维护,每次交换都是管理者和代理之间的一个独立的传送。

3. 陷阱引导轮询

如果管理者负责大量的代理,而每个代理又维护大量的对象,则靠管理者及时地轮询所有代理维护的所有可读数据是不现实的,因此管理者采取陷阱引导轮询技术对 MIB 进行控制和管理。

所谓陷阱引导轮询技术是:在初始化时,管理者轮询所有知道关键信息的代理;一旦建立了基准,管理者将降低轮询频度。相反地,由每个代理负责向管理者报告异常事件。例如,代理崩溃和重启动、连接失败、过载等,这些事件用 SNMP 的 Trap 报文报告。管理者一旦发现异常情况,可以直接轮询报告事件的代理或它的相邻代理,对事件进行诊断或获取关于异常情况的更多的信息。

陷阱引导轮询可以有效地节约网络容量和代理的处理时间。网络基本上不传送管理者不需要的管理信息,代理也不会无意义地频繁应答信息请求。

4. 代理

SNMP需要管理者及其所有代理支持UDP和IP,这限制了在不支持TCP/IP协议的设备上的应用。并且,大量的小系统虽然支持TCP/IP协议,但不希望承担维护SNMP、代理软件和MIB的负担。

为了兼容不支持SNMP的设备,SNMP提出了代理的概念。在这个模式下,一个SNMP的代理可以作为一个或多个其他设备的代理人。即管理者向代理发出对某个设备的查询操作,代理能够将查询转变为该设备使用的管理协议;当代理收到对一个查询的应答时,将这个应答转发给管理者。同样,如果一个来自托管设备的事件通报传到代理时,代理则以陷阱报文的形式将它发给管理者。

3.1.3 SNMP v1

1. SNMP v1支持的操作

SNMP只支持对管理对象值的检索和修改等简单操作,具体地,可以对MIB-2中的对象进行3.1.2节所述的Get、Set和Trap三种操作。MIB的结构不能通过增加或减少对象实例被改变,并且,访问只能对对象标识树中的叶子对象进行。这些限制大大简化了SNMP的实现,但同时也限制了网络管理系统的能力。

2. 共同体和安全控制

网络管理是一种分布式的应用,与其他分布式的应用相同,网络管理中包含由一个应用协议支持的多个应用实体的相互作用。在SNMP网络管理中,这些应用实体就是采用SNMP的管理者应用实体和被管理者的应用实体。

SNMP网络管理具有一些不同于其他分布式应用的特性,它包含一个管理者和多个被管理者之间一对多的关系。即管理者能够获取和设置各被管理者的对象,能够从各被管理者中接收陷阱信息。因此,从操作或控制的角度来看,管理者管理着多个被管理者。同时,系统中也可能有多个管理者,每个管理者都管理所有的或一部分被管理者。

反过来,SNMP网络管理中还包含另外一种一对多的关系——一个被管理者和多个管理者之间的关系。每个被管理者控制着自己的本地MIB,同时必须能够控制多个管理者对这个本地MIB的访问,这里所说的控制有以下三个方面的含义:

- 认证服务:将对MIB的访问限定在授权的管理者的范围内。
- 访问策略:对不同的管理者给予不同的访问权限。
- 代理服务:一个被管理者可以作为其他一些被管理者(托管站)的代理,这就要求在这个代理系统中实现为托管站服务的认证服务和访问权限。

以上这些控制都是为了保证网络管理信息的安全,即被管系统需要保护它们的MIB不被非法地访问。SNMP通过共同体的概念提供了初步的和有限的安全能力。

SNMP用共同体来定义一个代理和一组管理者之间的认证服务、访问控制和代理服务的关系。共同体是一个在被管系统中定义的本地的概念。被管系统为每组可选的认证服务、访问控制和代理服务建立一个共同体。每个共同体被赋予一个在被管系统内部唯一的共同体名,该共同体名要提供给共同体内的所有的管理者,以便它们在get和set操作中应用。代理可以与多个管理者建立多个共同体,同一个管理者可以出现在不同的共同体中。

由于共同体是在代理处本地定义的,因此不同的代理处可能会定义相同的共同体名。

共同体名相同并不意味着共同体有什么相似之处，因此，管理者必须将共同体名与代理联系起来加以应用。

（1）认证服务

认证服务是为了保证通信是可信的。在 SNMP 报文的情况下，认证服务的功能是保证收到的报文是来自它所声称的报文源。SNMP 只提供一种简单的认证模式，即所有由管理者发向代理的报文都包含一个共同体名，这个名字发挥口令的作用，如果发送者知道这个“口令”，则认为报文是可信的。

通过这种有限的认证形式，网络管理者可以对网络监控（set、trap），特别是网络控制（set）操作进行限制。共同体名被用于引发一个认证过程，而认证过程可以包含加密和解密以实现更安全的认证。

（2）访问策略

通过定义共同体，代理将对它的 MIB 的访问限定在了一组被选择的管理者中。通过使用多个共同体，代理可以为不同的管理者提供不同的 MIB 访问控制。访问控制包含以下两个方面：

- SNMP MIB 视图——MIB 中对象的一个子集。可以为每个共同体定义不同的 MIB 视图。视图中的对象子集可以不在 MIB 的一个子树之内。
- SNMP 访问模式——READ-ONLY 或 READ-WRITE。为每个共同体定义一个访问模式。

MIB 视图和访问模式的结合被称为 SNMP 共同体轮廓。即，一个共同体轮廓由代理处 MIB 的一个子集加上一个访问模式构成。SNMP 访问模式统一地被用于 MIB 视图中的所有对象。因此，如果选择了 READ-ONLY 访问模式，则管理者对视图中的所有对象都只能进行 read-only 操作。

事实上，在一个共同体轮廓之内，存在两个独立的访问限制——MIB 对象定义中的访问限制和 SNMP 访问模式。这两个访问限制在实际应用中必须得到协调。表 3-1 给出了这两个访问限制的协调规则。注意，对象被定义为 write-only，SNMP 也可以对其进行 read 操作。

表 3-1 MIB 对象定义中的 ACCESS 限制与 SNMP 访问模式的关系

MIB 对象定义中的 ACCESS 限制	SNMP 访问模式	
	read-only	read-write
read-only	get 和 trap 操作有效	
read-write	get 和 trap 操作有效	get、set 和 trap 操作有效
write-only	get 和 trap 操作有效，但操作值与具体实现有关	get、set 和 trap 操作有效，但操作值与具体实现有关
Not-accessible	无效	

在实际应用中，一个共同体轮廓要与代理定义的某个共同体联系起来，便构成了 SNMP 的访问策略。即 SNMP 的访问策略指出一个共同体中的 MIB 视图及其访问模式。

（3）代理服务

共同体的概念对支持代理服务也是有用的。如前所述，在 SNMP 中，代理是指为其他

设备提供管理通信服务的代理。对于每个托管设备,代理系统维护一个对它的访问策略,以此使代理系统知道哪些 MIB 对象可以被用于管理托管设备和能够用何种模式对它们进行访问。

3. SNMP 报文格式

管理者和代理之间以传送 SNMP 报文的形式交换信息。图 3-2 所示为封装成 UDP 数据报的 5 种操作的 SNMP 报文格式。可见一个 SNMP 报文共由三个部分组成,即公共 SNMP 首部、get/set 首部(trap 首部)、变量绑定。

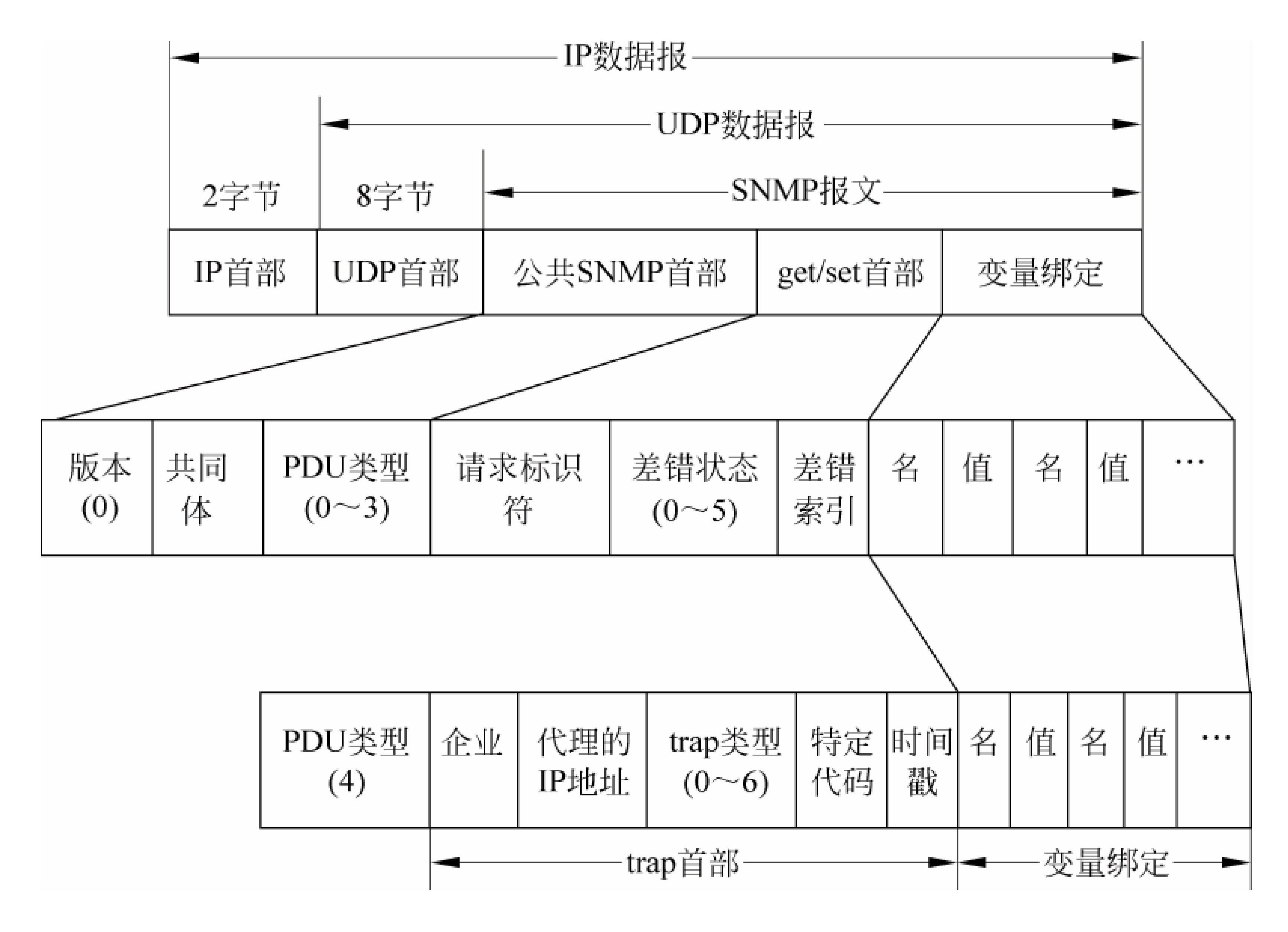


图 3-2　SNMP 报文格式

(1) 公共 SNMP 首部

公共 SNMP 首部包含以下字段:

- 版本——写入版本字段的是版本号减 1,对于 SNMP(即 SNMP v1)则应写入 0。
- 共同体——共同体就是一个字符串,作为管理进程和代理进程之间的明文口令,常用的是 6 个字符"public"。
- PDU 类型——根据 PDU 的类型,填入 0～4 中的一个数字,其对应关系如表 3-2 所示。

表 3-2　PDU 类型

PDU 类型	名　称	PDU 类型	名　称
0	get-request	3	set-request
1	get-next-request	4	trap
2	get-response		

(2) get/set 首部

get/set 首部包括以下字段:

- 请求标识符(request ID)——这是由管理进程设置的一个整数值,代理进程在发送 get-response 报文时也要返回此请求标识符。管理进程可同时向许多代理发出 get

报文，这些报文都使用 UDP 传送，先发送的有可能后到达。设置了请求标识符可使管理进程能够识别返回的响应报文对应于哪一个请求报文。

- 差错状态(error status)——由代理进程回答时填入 0～5 中的一个数字，各数字的含义见表 3-3 的描述。

表 3-3　差错状态描述

差错状态	名　　字	说　　明
0	noError	一切正常
1	tooBig	代理无法将回答装入到一个 SNMP 报文之中
2	noSuchName	操作指明了一个不存在的变量
3	badValue	一个 set 操作指明了一个无效值或无效语法
4	readOnly	管理进程试图修改一个只读变量
5	genErr	某些其他的差错

- 差错索引(error index)——当出现 noSuchName、badValue 或 readOnly 的差错时，由代理进程在回答时设置的一个整数，它指明有差错的变量在变量列表中的偏移。

(3) trap 首部

trap 首部包括以下字段：

- 企业(enterprise)：填入 trap 报文的网络设备的对象标识符。此对象标识符肯定是在图 2-2 的对象命名树上的 enterprise 节点{1.3.6.1.4.1}下面的一棵子树上。
- 代理的 IP 地址：该字段由 SNMP 代理填写，用来指明陷阱的发送者。
- trap 类型：此字段正式的名称是 generic-trap，共分为表 3-4 中的 7 种类型。

表 3-4　trap 类型描述

trap 类型	名　　字	说　　明
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	linkUp	一个接口从故障状态变为工作状态
4	authenticationFailure	从 SNMP 管理进程接收到具有一个无效共同体的报文
5	egpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	enterpriseSpecific	代理自定义的事件，需要用后面的“特定代码”来指明

当使用上述类型 2、3、5 时，在报文后面变量部分的第一个变量应标识响应的接口。

- 特定代码(specific-code)——指明代理自定义的时间(若 trap 类型为 6)，否则为 0。
- 时间戳(timestamp)——指明自代理进程初始化到 trap 报告的事件发生所经历的时间，单位为 ms。例如时间戳为 1908 表明在代理初始化后 1908ms 发生了该事件。

(4) 变量绑定(variable-bindings)

指明一个或多个变量的名和对应的值，在 get 或 get-next 报文中，变量的值应忽略。

4. 报文应答序列

SNMP 报文在管理者和代理之间传送，包含 GetRequest、GetNextRequest 和 SetRequest 的报文由管理者发出，代理以 GetResponse 响应。Trap 报文由代理发给管理

者,不需要应答,所有报文发送和应答序列如图3-3所示。一般来说,管理者可连续发出多个请求报文,然后等待代理返回的应答报文。如果在规定的时间内收到应答,则按照请求标识进行配对,亦即应答报文必须与请求报文有相同的请求标识。

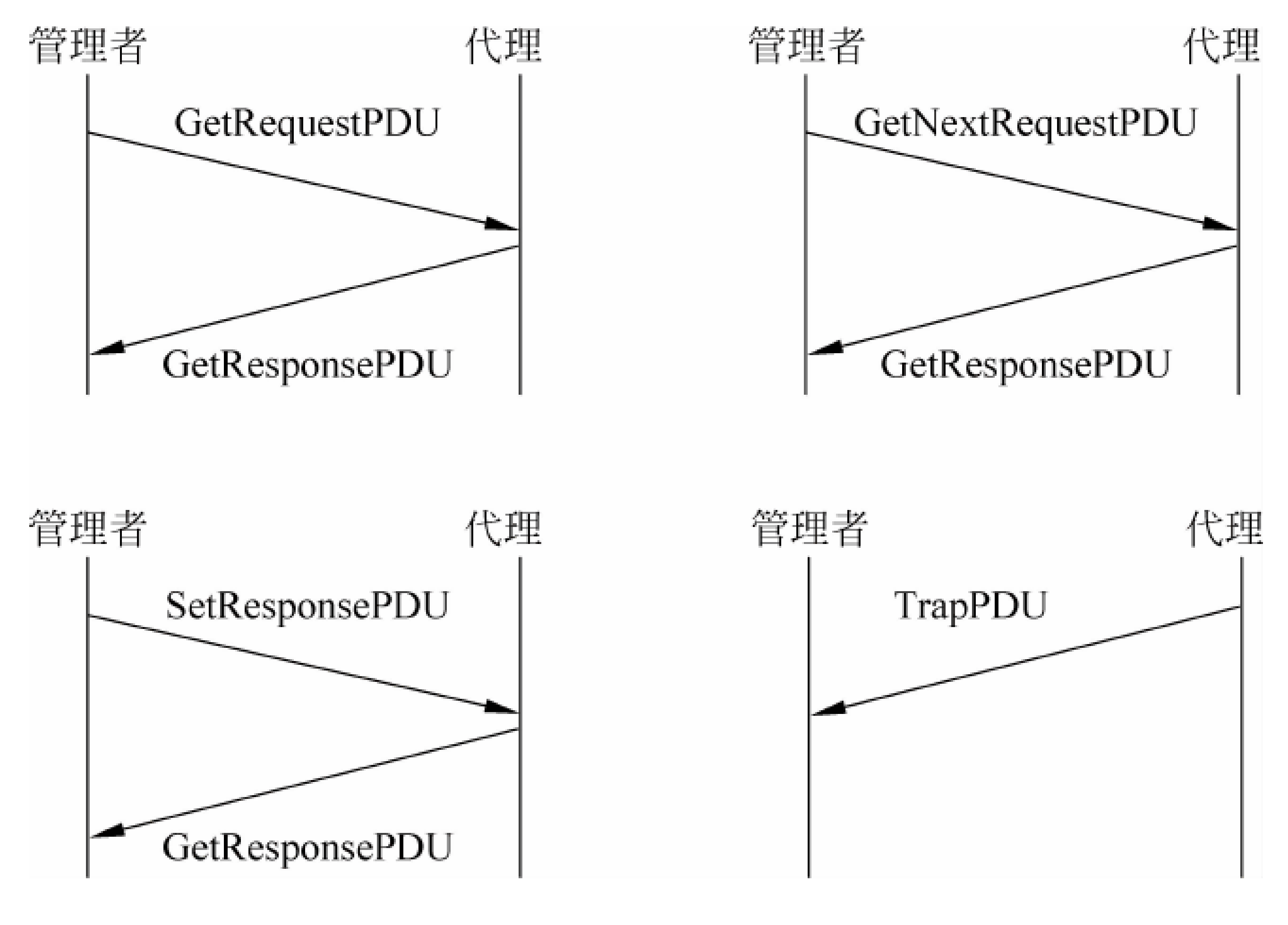


图3-3 SNMP报文应答序列

(1) GetRequest PDU

GetRequest PDU是由管理者应用程序发出的,发送实体将以下字段包含在PDU之中:

- PDU类型——指出GetRequest PDU类型。
- request-id——request-id能够使SNMP应用将得到的各个应答与发出的各个请求一一对应起来。同时也可以使SNMP实体能够处理由于传输服务的问题而产生的重复的PDU。
- variablebindings——要求获取值的对象实例清单。

GetRequest PDU的SNMP接收实体用包含相同request-id的GetResponse PDU进行应答。GetRequest操作是原子操作,即要么所有的值都提取回来,要么一个都不提取。但SNMP只允许提取MIB树中的叶子对象的值。因此不能只提供一个表或一个条目的名字来获取整个表或整行的对象值。但是可以将表中每行的各个对象包含在变量绑定中,来一次获取一行的对象值。

(2) GetNextRequest PDU

GetNextRequest PDU几乎与GetRequest PDU相同,GetNextRequest操作也是原子的。它们具有相同交换模式和相同的格式,唯一的不同是在GetRequest PDU中,变量绑定字段中列出的是要取值的对象实例名本身,而在GetNextRequest PDU中,变量绑定字段列出的是要取值的对象实例的"前一个"对象实例名。

虽然与GetRequest的外在差异不大,但是GetNextRequest却有GetRequest无法替代的用途。它能够使网络管理者去动态地发现一个MIB视图的结构,它也为查找不知其条目的表提供了一个有效的机制。

(3) SetRequest PDU

SetRequest PDU由管理者应用程序发出,与GetRequestPDU具有相同的交换模式和

相同的格式，SetRequest 操作也是原子的。但是，SetRequest 是被用于写对象值而不是读。因而，变量绑定清单中既包含对象实例标识符，也包含每个对象实例将被赋予的值。

SetRequest PDU 的 SNMP 接收实体用包含相同 request-id 的 GetResponsePDU 进行应答。如果应答实体能够更新变量绑定中的所有变量，则 GetResponsePDU 中包含提供给各个变量的值的变量绑定字段。只要有一个变量值不能成功地设置，则无变量值返回，也无变量值被更新。

利用 SetRequest 不仅可以对叶子对象实例进行值的更新，也可以利用变量绑定字段进行表格的行增加和行删除操作。

除此之外，SetRequest 还可被用于完成某种动作。SNMP 没有提供一种命令代理完成某种动作的机制，它的全部能力就是在一个 MIB 视图内 get 和 set 对象值，但是利用 set 的功能可以间接地发布完成某种动作的命令。某个对象可以代表某个命令，当它被设置为特定值时，就执行特定的动作。例如代理可以设一个初始值为 0 的对象 reBoot，如果管理者将这个对象值置 1，则代理系统被重新启动，reBoot 的值也被重新置 0。

（4） Trap PDU

TrapPDU 是由代理应用程序发出的，它被用于向管理者异步地通报某个重要事件。它的格式与其他的 SNMP PDU 完全不同，所包含的字段如下：

- PDU 类型——指出 TrapPDU 类型。
- enterprise——标识产生本 trap 的网络管理子系统（用 system 组中的 sysObjectId 值）。
- agent-addr——产生本 trap 的对象的 IP 地址。
- generic-trap——一种预定义的 trap。
- specific-trap——更明确地指出 trap 特性的代码。
- time-stamp——发出 trap 的网络实体从上次重启到产生本 trap 所经历的时间。
- variablebindings——有关 trap 的附加信息（本字段的意义与具体实现有关）。

5. 报文的发送与接收过程

（1） 报文发送

一般情况下，一个 SNMP 协议实体完成以下动作向其他 SNMP 实体发送 PDU：

① 构成 PDU。

② 将构成的 PDU、源和目的传送地址以及一个共同体名传给认证服务。认证服务完成所要求的变换，例如进行加密或加入认证码，然后将结果返回。

③ SNMP 协议实体将版本字段、共同体名以及上一步的结果组合成为一个报文。

④ 用基本编码规则（BER）对这个新的 ASN.1 的对象编码，然后传给传输服务。

（2） 报文接收

一般情况下，一个 SNMP 协议实体完成以下动作接收一个 SNMP 报文：

① 进行报文的基本句法检查，丢弃非法报文。

② 检查版本号，丢弃版本号不匹配的报文。

③ SNMP 协议实体将用户名、报文的 PDU 部分以及源和目的传输地址传给认证服务。如果认证失败，认证服务通知 SNMP 协议实体，由它产生一个 trap 并丢弃这个报文；如果认证成功，认证服务返回 SNMP 格式的 PDU。

④ 协议实体进行 PDU 的基本句法检查，如果非法，丢弃该 PDU；否则利用共同体名选

择对应的 SNMP 访问策略，对 PDU 进行相应处理。

在 SNMP 中，可以将多个同类操作(get、set、trap)放在一个报文中。如果管理者希望得到一个代理处的一组标量对象的值，它可以发送一个报文请求所有的值，并通过获取一个应答得到所有的值。这样可以大大减少网络管理的通信负担。

为了实现多对象交换，所有的 SNMP 的 PDU 都包含了一个变量绑定字段。这个字段由对象实例的一个参考序列及这些对象的值构成。某些 PDU 只需给出对象实例的名字，如 get 操作，对于这样的 PDU，接收协议实体将忽略变量绑定字段中的值。

3.1.4 SNMP v2

1. SNMP v2 对 SNMP v1 的改进

1993 年，SNMP 的改进版 SNMP v2 开始发布，最初的 SNMP v2 最大的特色是增加了安全特性，因此被称为安全版 SNMP v2。但不幸的是，经过几年试用，没有得到厂商和用户的积极响应，并且也发现自身还存在一些严重缺陷。因此，在 1996 年正式发布的 SNMP v2 中，安全特性被删除。这样，SNMP v2 对 SNMP v1 的改进程度便受到了很大的削弱。

总的来说，SNMP v2 的改进主要有以下 3 个方面：

- 支持分布式管理。
- 改进了管理信息结构。
- 增强了管理信息通信协议的能力。

SNMP v1 采用的是集中式网络管理模式，网络管理者的角色由一个主机担当，其他设备(包括代理软件和 MIB)都由管理者监控。随着网络规模和业务负荷的增加，这种集中式的系统已经不再适应需要。管理者的负担太重，并且来自各个代理的报告在网上产生大量的业务量。而 SNMP v2 不仅可以采用集中式的模式，而且也可以采用分布式模式。在分布式模式下可以有多个顶层管理者，被称为管理服务器。每个管理服务器可以直接管理代理，同时，管理服务器也可以委托中间管理者担当管理者角色监控一部分代理。对于管理服务器，中间管理者又以代理的身份提供信息和接受控制。这种体系结构分散了处理负担，减小了网络的业务量。

SNMP v2 在几个方面对 SNMP v1 的 SMI 进行了扩充。定义对象的宏中包含了一些新的数据类型。最引人注目的变化是提供了对表中的行进行删除或建立操作的规范。新定义的 SNMP v2 MIB 包含有关 SNMP v2 协议操作的基本流量信息和有关 SNMP v2 管理者和代理的配置信息。

在通信协议操作方面，最引人注目的变化是增加了两个新的 PDU——GetBulkRequest 和 InformRequest。前者使管理者能够有效地提取大块的数据，后者使管理者能够向其他管理者发送 trap 信息。

2. SNMP v2 网络管理框架

SNMP v2 提供了一个建立网络管理系统的框架。但网络管理应用，如故障管理、性能监测、计费等不包括在 SNMP v2 的范围内。用术语来说，SNMP v2 提供的是网络管理基础结构。

SNMP v2 本质上是一个交换管理信息的协议，网络管理系统中的每个角色都维护一个与网络管理有关的 MIB。SNMP v2 的 SMI 对这些 MIB 的信息结构和数据类型进行定义，

SNMP v2 提供了一些一般的通用的 MIB，厂商或用户也可以定义自己私有的 MIB。

在配置中至少有一个系统负责整个网络的管理，这个系统就是网络管理应用驻留的地方。管理者可以设置多个，以便提供冗余或分担大网络的管理责任。其他系统担任代理角色，代理收集本地信息并保存，以备管理者提取。这些信息包括系统自身的数据，也可以包括网络的业务量信息。

SNMP v2 既支持高度集中化的网络管理模式，也支持分布式的网络管理模式。在分布式模式下，一些系统担任管理者和代理两种角色，这种系统被称为中间管理者。中间管理者以代理身份从上级管理系统接受被管理信息操作命令，如果这些命令所涉及的管理信息在本地 MIB 中，则中间管理者便以代理身份进行操作并进行应答，如果所涉及的管理信息在中间管理者的下属代理的 MIB 中，则中间管理者先以管理者身份对下属代理进行发布操作命令，接收应答，然后再以代理身份向上级管理者应答。

所有这些信息交换都利用 SNMP v2 通信协议实现。与 SNMP v1 相同，SNMP v2 协议仍是一个简单的 request/response 型协议，但在 PDU 种类和协议功能方面对 SNMP v1 进行了扩充。

3. 协议操作

(1) SNMP v2 报文

与 SNMP v1 相同，SNMP v2 以包含协议数据单元(PDU)的报文的形式交换信息。外部的报文结构中包含一个用于认证的共同体名。

SNMP v2 确定的报文结构如下：

```
Message ::= SEQUENCE {
        version        INTEGER { version (1) },   -- SNMP v2 的版本号为 1
        community      OCTET STRING,              -- 共同体名
        data           ANY                        -- SNMP v2 PDU
        }
```

SNMP v2 报文的发送和接收过程与 SNMP v1 报文的发送和接收过程相同。

(2) PDU 格式

在 SNMP v2 报文中可以传送 7 类 PDU，表 3-5 列出了这些 PDU，同时指出了对 SNMP v1 也有效的 PDU。图 3-4 描述了 SNMP v2 PDU 的一般格式。

表 3-5　SNMP 协议数据单元(PDU)

PDU	描　　述	SNMP v1	SNMP v2
Get	管理者通过代理获得每个对象的值	○	○
GetNext	管理者通过代理获得每个对象的下一个值	○	○
GetBulk	管理者通过代理获得每个对象的 N 个值		○
Set	管理者通过代理为每个对象设置值	○	○
Trap	代理向管理者传送随机信息	○	○
Inform	管理者向代理传送随机信息		○
Response	代理对管理者的请求进行应答	○	○

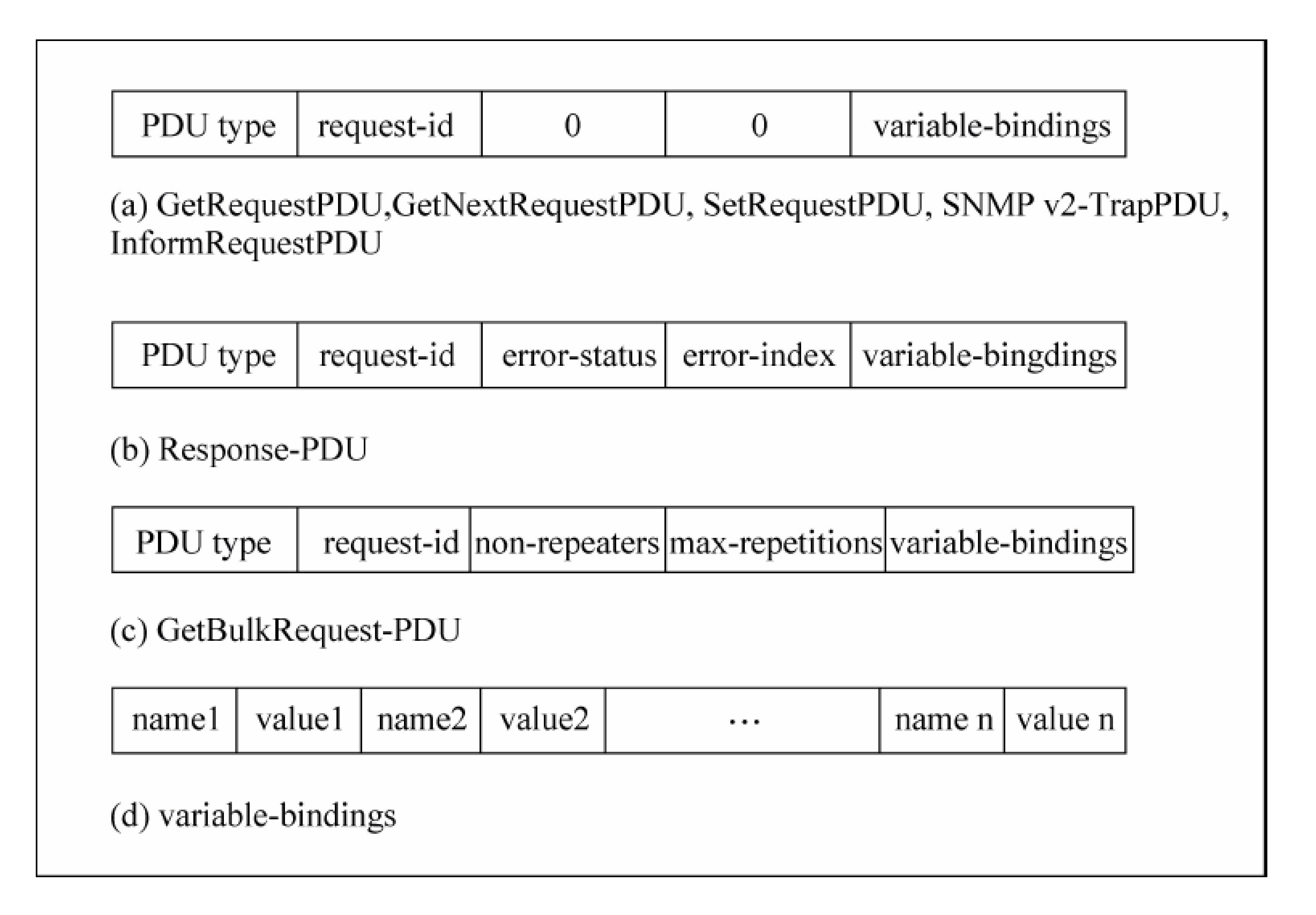


图 3-4　SNMP v2 PDU 格式

值得注意的是，GetRequest、GetNextRequest、SetRequest、SNMP v2-Trap、InformRequest 5 种 PDU 具有完全相同的格式，并且也可以看作是 error-status 和 error-index 两个字段被置零的 Response PDU 的格式。这样设计的目的是减少 SNMP v2 实体需要处理的 PDU 格式种类。

① GetRequest PDU

SNMP v2 的 GetRequest PDU 的语法和语义都与 SNMP v1 的 GetRequest PDU 相同，差别是对应答的处理。SNMP v1 的 GetRequest 操作是原子的，而 SNMP v2 能够部分地对 GetRequest 操作进行应答。即使有些变量值提供不出来，变量绑定字段也要包含在应答的 GetResponse PDU 之中。如果某个变量有意外情况（noSuchObject、noSuchInstance、endOfMibView），则在变量绑定字段中，这个变量名与一个代表意外情况的错误代码而不是变量值配对。

在 SNMP v2 中，按照以下规则处理 GetRequest 变量绑定字段中的每个变量来构造应答 PDU：

- 正常情况下，值字段被设置为变量值。
- 如果 OBJECT IDENTIFIER 前缀与该请求在代理处所能访问的变量的前缀都不匹配，则它的值字段被设置为 noSuchObject；否则，如果变量名与该请求在代理处所能访问的变量的名称都不匹配，则它的值字段被设置为 noSuchInstance。
- 如果由于其他原因导致变量名处理过程的失败，则无法返回变量值。这时，应答实体将返回一个 error-status 字段值为 genErr，并在 error-index 字段中指出问题的变量的应答 PDU。
- 如果生成的应答 PDU 中的报文过大，超过了指定的最大限度，则生成的 PDU 被丢弃，并用一个 error-status 字段值为 tooBig、error-index 字段值为 0、变量绑定字段为空的新的 PDU 应答。

允许部分应答是对 GetRequest 的重要改进。在 SNMP v1 中，只要有一个变量值取不

回来，所有的变量值就都不能返回。在这种情况下，发出操作请求的管理者往往只能将命令拆分为多条只取单个变量值的命令。相比之下，SNMP v2 的操作效率得到了很大提高。

② GetNextRequest PDU

SNMP v2 的 GetNextRequest PDU 的语法和语义都与 SNMP v1 的 GetNextRequest PDU 相同。与 GetRequestPDU 相同，两个版本的差别是对应答的处理，SNMP v1 的 GetNextRequest 操作是原子的，而 SNMP v2 能够部分地对 GetNextRequest 操作进行应答。

在 SNMP v2 中，按照以下规则处理 GetNextRequest 变量绑定字段中的每个变量来构造应答 PDU：

- 确定被指名的变量存在下一个变量，将该变量名和它的值成对地放入结果变量绑定字段中。
- 如果被指定的变量之后不存在变量，则将被指定的变量名和错误代码 endOfMibView 成对地放入结果变量绑定字段中。
- 如果由于其他原因导致变量名处理过程的失败，或者是产生的结果太大，处理过程与 GetRequest 相同。

③ GetBulkRequest PDU

SNMP v2 的一个主要改进是 GetBulkRequest PDU，这个 PDU 的目的是尽量减少查询大量管理信息时所进行的协议交换次数，GetBulkRequest PDU 允许 SNMP v2 管理者请求得到在给定的条件下尽可能大的应答。GetBulkRequest 操作利用与 GetNextRequest 相同的选择原则，即总是顺序选择下一个对象。不同的是，利用 GetBulkRequest 可以选择多个后继对象。

GetBulkRequest 操作的基本工作过程为：GetBulkRequest 在变量绑定字段中放入一个（N＋R）个变量名的清单。对于前 N 个变量名，查询方式与 GetNextRequest 相同，即对清单中的每个变量名，返回它的下一个变量名和它的值，如果没有后继变量，则返回原变量名和一个 endOfMibView 的值。

GetBulkRequest PDU 有两个其他 PDU 所没有的字段 non-repeaters 和 max-repetitions。non-repeaters 字段指出只返回一个后继变量的变量数；max-repetitions 字段指出其他的变量应返回的最大的后继变量数。

GetBulkRequest 操作解除了 SNMP 的一个主要限制，即不能有效地检索大块数据。此外，利用这个功能可以减小管理应用程序的规模。管理应用程序自身不需要关心组装在一起的请求的细节，不需要执行一个试验过程来确认请求 PDU 中的 name-value 对的最佳数量。并且，即使 GetBulkRequest 发出的请求过大，代理也会尽量多地返回数据而不是简单地返回一个 tooBig 的错误报文。为了获得缺少的数据，管理者只需简单地重发请求，而不必将原来的请求改装为小的请求序列。

④ SetRequest PDU

SetRequest PDU 由管理者发出，用来请求改变一个或多个对象的值。接收实体用一个包含相同 request-id 的 Response PDU 应答。与 SNMP v1 相同，SetRequest 操作也是原子的。如果接收实体能够为被指名的所有变量设置新值，则 Response PDU 返回与 SetRequest 相同的变量绑定字段。只要有一个变量值没设置成功，就不更新任何值。

SetRequest 的变量绑定分为确认每个绑定对和更新在变量绑定字段中被指名的所有的变量两个阶段。

在第一阶段中，需要对每个绑定对进行确认，直至所有的绑定对都成功或遇到一个失败为止。如果失败，则返回一个在 error-status 字段给出的错误代码，在 error-index 字段给出有问题的变量的序号的应答 PDU。如果在确认阶段没有遇到问题，则进入第二阶段。

在第二阶段中，不存在的变量需要建立，存在的变量被赋予新值。只要遇到任何失败，则所有的更新都被撤销，并返回一个 error-status 字段值为 commitFailed 的 Response PDU。

⑤ SNMP v2 Trap PDU

SNMP v2 Trap PDU 由一个代理实体在发现异常事件时产生并发给管理者。与 SNMP v1 相同，它用于向管理者提供一个异步的通报以便报告重要事件。但它的格式与 SNMP v1 不同，与 GetRequest、GetNextRequest、GetBulkRequest、SetRequest 和 InformRequest PDU 拥有相同的格式。变量绑定字段用于容纳与陷阱报文有关的信息。Trap PDU 是一个非认证报文，不要求接收实体应答。

⑥ InformRequest PDU

InformRequest PDU 由一个管理者角色的 SNMP v2 实体应它的应用请求发给另一个管理者角色的 SNMP v2 实体，请求后者向某个应用提供管理信息。与 SNMP v2 Trap PDU 类似，变量绑定字段被用于传送相关的信息。

收到 InformRequest 的实体首先检查承载应答 PDU 的报文大小，如果报文超过限度，用一个含有 tooBig 错误代码的 Response PDU 应答。否则，接收实体将 PDU 中的内容转到信息的目的地，同时对发出 InformRequest 的管理者用 error-status 字段值为 noError 的 Response PDU 进行应答。

3.1.5 SNMP v3

SNMP v3 在 SNMP v2 基础之上增加、完善了安全和管理机制。SNMP v3 体系结构体现了模块化的设计思想，使管理者可以简单地实现功能的增加和修改。其主要特点在于适应性强，可适用于多种操作环境，不仅可以管理最简单的网络，实现基本的管理功能，还能够提供强大的网络管理功能，满足复杂网络的管理需求。

1. SNMP v3 的新特性

SNMP v3 增加一些新特性，最引人注目的新特性是：Getbulk 操作、64 位计数器、增强了的 set 命令，以及为每个 SNMP 引擎分配的独特的 ID 号等。这些新特性适应了网络技术的进步，并扩展了老协议的某些局限性。而且，SNMP v3 完善了一些协议的操作，当查询代理中的大量数据时，Getbulk 操作可以把多个 get 和 Getnext 操作连接到一个包内，这样可以减少传输过程中的碰撞效应。SNMP v3 在执行 set 操作后，通过一个查询来测试 set 操作是否成功，从而保证其有效性。这个最新的 SNMP 版本同时也改进了 SNMP 管理框架本身的一些结构。此外，SNMP v3 还增加了一个 snmpEngineID，它能从一个管理设备上定位其他设备上的多种上下文。

这些新特性使管理者能在网络拓扑结构中跟踪各种关系，有助于在一个管理设备中鉴别和定位更复杂的网络基础部件。

2. SNMP v3 的体系结构

SNMP v3 主要有三个模块：信息处理和控制模块、本地处理模块和用户安全模块。

(1) 信息处理和控制模块

信息处理和控制模块(Message Processing And Control Model)在 RFC 2272 中定义，它负责信息的产生和分析，并判断信息在传输过程中是否要经过代理服务器等。在信息产生过程中，该模块接收来自调度器(Dispatcher)的 PDU，然后由用户安全模块在信息头中加入安全参数。在分析接收的信息时，先由用户安全模块处理信息头中的安全参数，然后将解包后的 PDU 送给调度器处理。

(2) 本地处理模块

本地处理模块(Local Processing Model)的功能主要是进行访问控制，处理打包的数据和中断。访问控制是指通过设置代理的有关信息使不同的管理者的管理进程在访问代理时具有不同的权限，它在 PDU 这一级完成。常用的控制策略有两种：限定管理者可以向代理发出的命令或确定管理者可以访问代理的 MIB 的具体部分。访问控制的策略必须预先设定，SNMP v3 通过使用带有不同参数的原语来灵活地确定访问控制方式。

(3) 用户安全模块

与 SNMP v1 和 SNMP v2 相比，SNMP v3 增加了三个新的安全机制：身份验证，加密和访问控制。其中，本地处理模块完成访问控制功能，而用户安全模块(User Security Model)则提供身份验证和数据加密服务。身份验证是指代理(管理者)接到信息时首先必须确认信息是否来自有权的管理者(代理)，并且信息在传输过程中未被改变的过程。实现这个功能要求管理者和代理必须共享同一密钥。管理者使用密钥计算验证码，然后将其加入信息中，而代理则使用同一密钥从接收的信息中提取出验证码，从而得到信息。加密的过程与身份验证类似，也需要管理者和代理共享同一密钥来实现信息的加密和解密。

3. SNMP 实体

SNMP v3 的一个目标是支持一种容易扩展的模块化体系结构，将以前版本中的代理和管理者统一为 SNMP 实体。SNMP 实体由两部分组成：SNMP 引擎和 SNMP 应用程序。SNMP 实体是体系结构的一个实现，每个 SNMP 实体都由一个 SNMP 引擎和一个或多个有关的 SNMP 应用组成，图 3-5 显示了 SNMP 实体的组成元素。

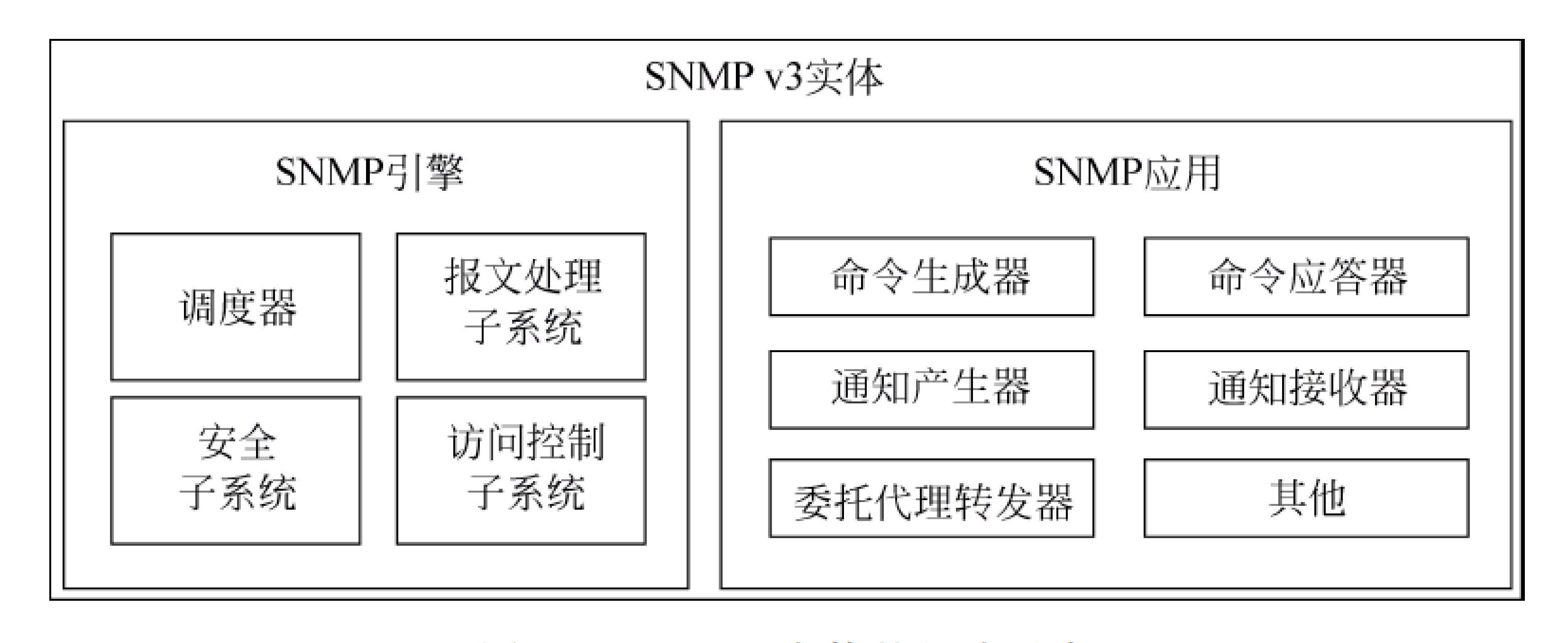


图 3-5　SNMP 实体的组成元素

SNMP 引擎为发送和接收报文、认证和加密报文、控制对被管对象的访问提供服务。SNMP 引擎与包含它的 SNMP 实体之间存在一对一的联系。SNMP 引擎中包括：调度器

(Dispatcher)、报文处理子系统(Message Processing Subsystem)、安全子系统(Security Subsystem)和访问控制子系统(Access Control Subsystem)。

在一个管理域中,每个 SNMP 引擎都有一个唯一的和明确的标识符(snmpEngingID)。由于引擎和实体之间一一对应,因此 snmpEngingID 也能在管理域中唯一地、明确地标识实体。但是,在不同的管理域中,SNMP 的实体可能会有相同的 snmpEngineID。

一个 SNMP 引擎中只有一个调度器,但能够同时支持多个版本的 SNMP 报文。它的功能包括:

- 向网络发送或从网络接收 SNMP 报文。
- 确定 SNMP 报文的版本,与相应的报文处理模型相互作用。
- 为 SNMP 应用提供抽象接口,用以向应用传递 PDU。
- 为 SNMP 应用提供抽象接口,用以允许它们向远程 SNMP 实体发送 PDU。

4. 报文处理子系统

报文处理子系统负责准备要发送的报文和从收到的报文中抽取数据。如图 3-6 所示,报文处理子系统由一个或多个报文处理模块组成。



图 3-6　报文处理子系统

每个报文处理模块定义一个特定版本的 SNMP 报文的格式,对应所定义的格式对准备和抽取处理进行相应的调整。这种体系结构也允许扩充其他的报文处理模块,扩充的处理模块可以是企业专用的,也可以是以后的标准增添的。

5. 安全子系统

安全子系统提供诸如报文的认证和隐私的安全服务。一个安全子系统可以有多个安全模块,以便提供各种不同的安全服务。

从体系结构上来讲,安全子系统由安全模型和安全协议组成,每一个安全模块定义了一种具体的安全模型,指明了它所防范的威胁、服务的目标和为提供安全服务所采用的安全协议,如认证和隐私。安全协议指出为提供安全服务所采用的机制、过程和 MIB 对象。目前的标准提供了基于用户的安全模型,如图 3-7 所示。



图 3-7　安全子系统

SNMP v3 的安全目标是:

- 能够验证 SNMP 报文的完整性,确认在传输的过程中是否被篡改。
- 能够鉴别报文发送者的身份,识破伪装者。
- 可以查询报文的生成时间,确认从发送到接收的延迟是否在限定的时间内。

为了实现上述目标,RFC2574 把安全协议分为认证模块、时间序列模块和加密模块三个模块。认证模块用于数据完整性鉴别和数据源身份认证;时间序列模块用于检验报文的传输时延,确认其在规定的时间窗口内;加密模块实现对报文内容的加密。

6. 访问控制子系统

访问控制子系统通过一个或多个访问控制模块提供授权服务。每个访问控制模块定义一个特定的访问决策函数，用以支持对访问权限的决策。在应用程序处理的过程中，访问控制模块还可以通过已定义的 MIB 模块进行远程配置访问控制策略。目前，基于视图的访问控制模型的访问控制模块是 SNMP v3 所建议的，如图 3-8 所示。

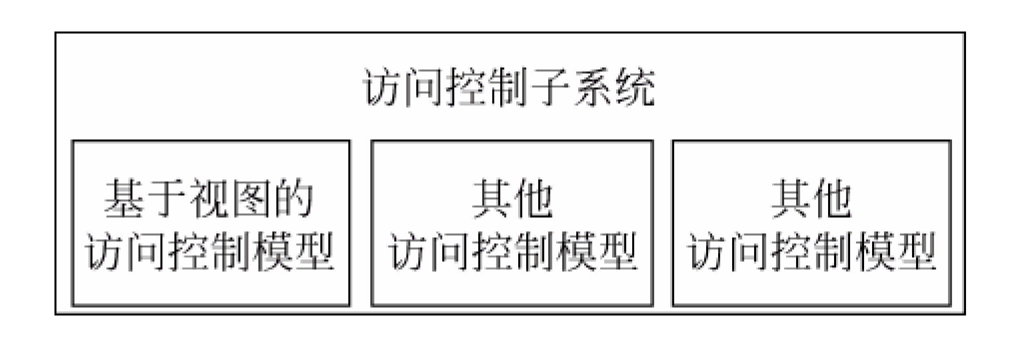


图 3-8　访问控制子系统

3.2　公共管理信息协议

3.2.1　CMIP/CMIS 概述

公共管理信息协议(Common Management Information Protocol，CMIP)协议是在 OSI 制订的网络管理框架中提出的网络管理协议，所提供的服务是公共管理信息服务(Common Management Information Service，CMIS)。CMIP 包含以下组成部分：一套用于描述协议的模型，一组用于描述被管对象的注册、标识和定义的管理信息结构，被管对象的详细说明以及用于远程管理的原语和服务。CMIP 与 SNMP 一样，也是由被管代理和管理者、管理协议与管理信息库组成。在 CMIP 中，被管代理和管理者没有明确的指定，任何一个网络设备既可以是被管代理，也可以是管理者。

CMIP 管理模型可以用三种模型进行描述：组织模型用于描述管理任务如何分配；功能模型用于描述各种网络管理功能和它们之间的关系；信息模型提供了描述被管对象和相关管理信息的准则。从组织模型来说，所有 CMIP 的管理者和被管代理存在于一个或多个域中，域是网络管理的基本单元。从功能模型来说，CMIP 主要实现故障管理、配置管理、性能管理、记账管理和安全性管理。每种管理均由一个特殊管理功能领域(Special Management Functional Area，SMFA)负责完成。从信息模型来说，CMIP 的 MIB 是面向对象的数据存储结构，每一个功能领域以对象为 MIB 的存储单元。

CMIP 是一个完全独立于下层平台的应用层协议，它的五个特殊管理功能领域由多个系统管理功能(SMF)加以支持。相对来说，CMIP 是一个相当复杂和详细的网络管理协议。它的设计宗旨与 SNMP 相同，但用于监视网络的协议数据报文要相对多一些。CMIP 共定义了 11 类 PDU。在 CMIP 中，变量以非常复杂和高级的对象形式出现，每一个变量包含变量属性、变量行为和通知。CMIP 中的变量体现了 CMIP MIB 的特征，并且这种特征表现了 CMIP 的管理思想，即基于事件而不是基于轮询。每个代理独立完成一定的管理工作。

3.2.2　CMIS 的实现

OSI 网络管理协议的整体结构建立在假设使用了 OSI 参考模型的基础上，网络管理应用进程使用 OSI 参考模型中的应用层。也是在这一层，公共管理信息服务元素(CMISE)提供了应用程序使用 CMIP 的手段。在第 7 层中又包含了两个 OSI 应用协议：联系控制服务元素(Association Control Service Element，ACSE)和远程操作服务元素(Remote Operation

Service Element,ROSE)。ACSE 用于在应用程序之间建立和关闭联系;ROSE 用于处理应用之间的请求/应答交互。

OSI 参考模型中,第 1 层到第 6 层对网络管理的贡献是为管理信息的传递提供标准的信息传输服务,在应用层上则要有特定的网络管理应用服务以支持网络管理通信。在 OSI 网络管理标准中,应用层上与网络管理应用有关的实现称为系统管理应用实体。

通过协议在两个实体(管理者与代理)之间进行管理信息的交换是 ISO 提出的网络管理的基本功能,这种功能被称为公共管理信息服务元素(Common Management Information Service Element,CMISE)。CMISE 的定义分为两部分:

- CMIS——描述提供给用户的服务。
- CMIP——描述完成 CMIS 服务的 PDU 的格式及其相关联的过程。

在 OSI 管理信息通信中,管理进程和管理代理是两个对等的应用实体,它们调用 CMISE 的服务来交换管理信息。CMISE 提供的服务访问点支持管理进程和管理代理之间有控制的关联。关联用于管理信息的查询/响应、传递事件通知、远程启动管理对象的操作等。

CMISE 的管理信息通信需要面向连接的传输支持,并且和应用层环境有一定的关系。CMISE 利用了 OSI 联系控制服务元素(ACSE)和远程操作服务元素(ROSE)来实现它自己的管理信息服务。为了实现 CMIS/CMIP,有 3 个 OSI 应用层协议(也称为服务元素)必不可少:

- 公共管理信息服务元素(CMISE)——用于提供 CMIS 服务。
- 联系控制服务元素(ACSE)——用于建立和拆除两个系统之间应用层的通信联系。
- 远程操作服务元素(ROSE)——用于建立和释放应用层的链接。

CMISE 使用户能够访问到 CMIS 管理服务,该服务则利用 CMIP 作为其管理进程/代理进程的通信手段。CMISE 要用到 ACSE 和 ROSE 的支持,用于对应用联系的控制。ACSE 实现的是打开和关闭管理进程和代理进程之间的通信联系,而 ROSE 则在联系建立起来后传送请求和响应。

CMIS 定义了每个网络组成部分提供的网络管理服务。这些服务在本质上是一般的,而不是特有的,CMIP 是实现 CMIS 服务的协议。

OSI 网络协议意在为所有设备在 OSI 参考模型的每一层提供一个公共网络结构。同样,CMIS/CMIP 意在提供一个用于所有网络设备的完整网络管理协议簇。为了提供位于多种不同的网络机器和计算机结构之上所需的网络管理协议特征,CMIS/CMIP 的功能和结构远远不同于 SNMP。SNMP 是按照简单和易于实现的原则设计的。OSI 网络管理协议并不像 SNMP 一样过分简单化,它们能够提供支持一个完整的网络管理方案所需的功能。

3.3 基于 Web 的管理技术

3.3.1 WBM 概述

1. WBM 的产生

随着应用 Intranet 的企业的增多,一些主要的网络厂商正试图以一种新的形式去应用管理信息系统,从而进一步管理企业网络。WBM(Web-Based Management)技术允许管理

人员通过与 WWW 同样的能力监测他们的网络，这将使得大量的 Intranet 成为更加有效的通信工具。WBM 可以允许网络管理人员使用任何一种 Web 浏览器，在网络任何节点上方便迅速地配置、控制以及存取网络和它的各种部分。WBM 是网管方案的一次革命，它将使网络用户管理网络的方式得以改善。

2. WBM 的优势

WBM 融合了 Web 功能与网管技术，从而为网管人员提供了比传统工具更强有力的能力。管理人员应用 WBM 能够通过任何 Web 浏览器、在任何站点监测和控制企业网络，而不再只拘泥于网管工作站，并且由此能够解决很多由于多平台结构产生的互操作性问题。WBM 提供比传统的命令驱动远程登录屏幕更直接、更易用的图形界面，浏览器操作和 Web 页面对 WWW 来讲是非常熟悉的，所以 WBM 的结果必然是既降低了管理信息系统全体培训的费用，又促进了更多的用户去利用网络运行状态信息。

3.3.2 WBM 的实现方法

WBM 有两种基本的实现方法，它们之间平行地发展而且互不干涉。

1. 代理方式

代理方式也就是将一个 Web 服务器加到一个内部网络工作站（代理）上，如图 3-9 所示，这个工作站轮流与端设备通信，浏览器用户通过 HTTP 协议与代理通信，同时代理通过 SNMP 协议与端设备通信。一种典型的实现方法是提供商将 Web 服务器加到一个已经存在的网管设备上去。这样做可以平衡像数据库访问、SNMP 轮询等功能。

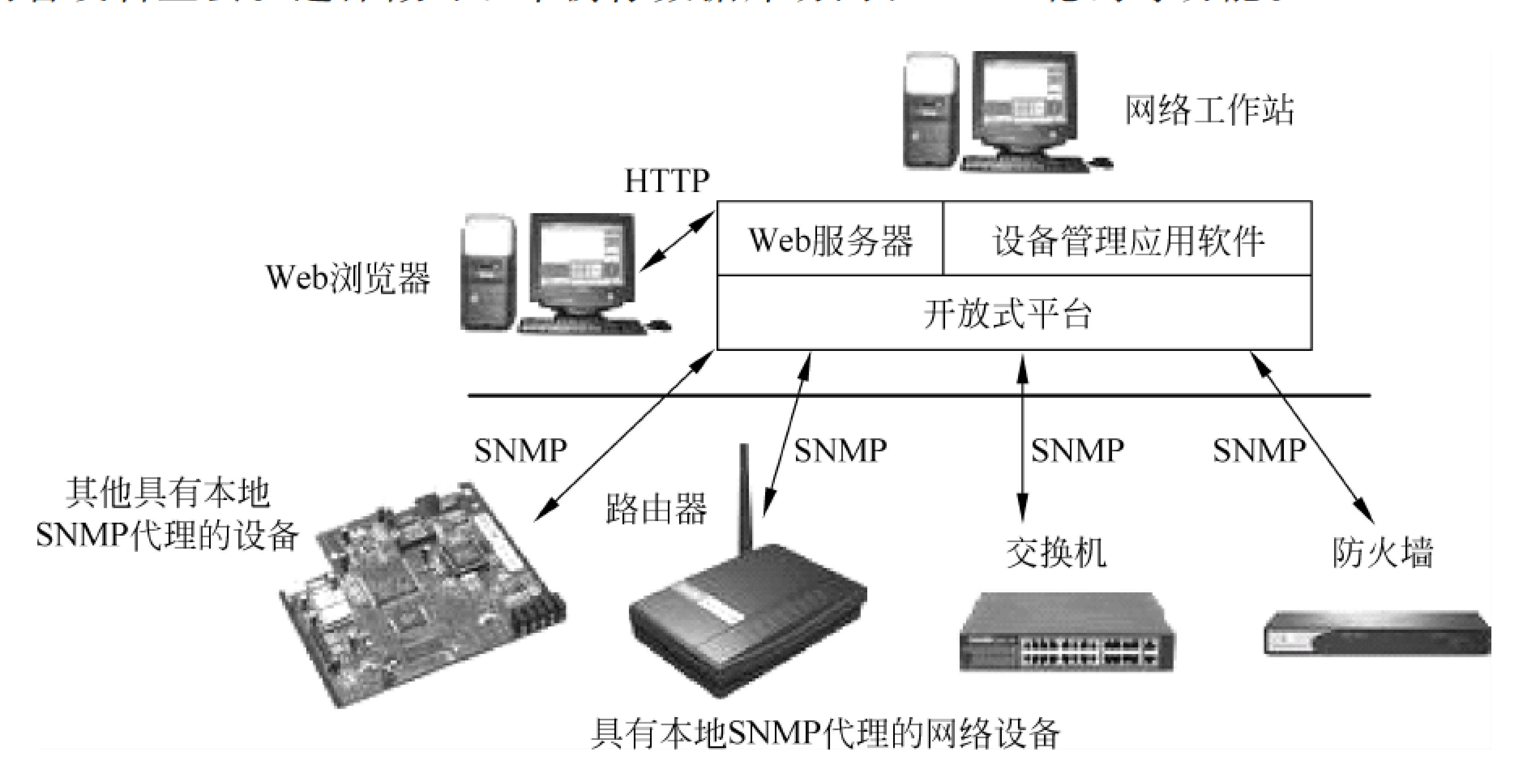


图 3-9 基于 Web 管理的典型方式

2. 嵌入方式

嵌入方式将 Web 能力真正地嵌入到网络设备中，每个设备有它自己的 Web 地址，管理人员可轻松地通过浏览器访问到该设备并且管理它，如图 3-10 所示。

代理方式保留了现存的基于工作站的网管系统及设备的全部优点，同时还增加了访问灵活的优点。既然代理与所有网络设备通信，那么它当然能提供一个企业的所有物理设备的全体映像，就像一个虚拟的网络那样。代理与设备之间的通信沿用 SNMP，所以这种方案的实施只需要那些“传统”的设备即可。



图 3-10　基于 Web 管理的嵌入方式

另一方面,嵌入方式给各独立设备带来了图形化的管理。这一点保障了非常简单易用的接口,它优于现在的命令行或基于菜单的远程登录界面,Web 接口可提供更简单的操作而不损失功能。

在未来的企业网络中,基于代理和基于嵌入方式的两种网管方案都将被应用。一个大型的机构可能需要继续通过所谓的代理方式来进行全部网络的监测与管理,而且代理方案也能够充分管理大型机构中的纯粹 SNMP 设备。与此同时,嵌入方式也将有着强大的生命力,例如这种方式在不断前进的界面以及在安装新设备时配置设备方面就极具优势。

嵌入方式对于小规模的环境也许更为理想,小型网络系统简单并且不需要强有力的管理系统以及企业全面视图。通常组织在网络和设备控制的培训方面比较不足,那么嵌入到每个设备的 Web 服务器将使用户从复杂的网管中解放出来。另外,基于 Web 的设备提供真正的即插即用安装,这将减少安装时间、故障排除时间。

3.3.3　WBM 的标准

开放标准是减轻网管复杂性和降低网络管理费用的必要条件,现在有两项 WBM 标准正处于考虑之中。一个是 WBEM(Web-Based Enterprise Management)标准,于 1996 年 7 月推出,WBEM 是 Microsoft 最先提出的,包括 3Com 在内的 60 多个提供商都支持此项标准。此项标准是面向对象的,能够将从多来源(设备、系统、应用程序)以多协议(例如 SNMP、DMI)获得的数据抽象化,它加强了管理能力,并且使它们通过单一的协议出现。

WBEM 被认为是"兼容和扩展"了当前的标准,如 SNMP、DMI 和 CMIP,并不是取而代之。虽然 WBEM 使自己以 Web 工具的形式出现,但它的真正目标是强化对于网络元素和系统的管理。WBEM 的关键是一个新的协议 HMMP(Hypermedia Management Protocol),这个传输协议处理包括重发功能、分组速率、传送证实以及允许一个报文拆成一个或几个分组等功能。

另一个 WBM 标准是 JMAPI(Java-Management Application Program Interface),它被作为 Sun 的 Java 标准扩展 API 结构的一部分。超过 JMAPI 本身的含义,JMAPI 其实是一个完整的网络管理应用程序开发环境,它提供了一个厂商当今不得不收集到的完全的特性清单,包括生成资源清单表格、图像的用户接口、SNMP 的网络 API、远程过程调用主机、数

据库访问方法以及式样向导。在理论上，JMAPI 的应用程序在整个 Web 上将以同样的界面和功能灵活地实现互操作。

3.4 本章小结

本章主要介绍了 SNMP 的发展、基本框架、格式、通信机制等内容。首先介绍了 SNMP 演化的过程，并对其基本结构框架、协议环境、基本应用配置等基础知识进行了介绍。接着分别介绍了 SNMP v1、SNMP v2、SNMP v3 的基本特点，并简单介绍了公共管理信息协议(GMIP)。最后介绍了基于 WBM 的网络管理思想。

SNMP 采用了基于 Client/Server 形式的管理者—代理模型，网络的管理与维护是通过管理者与代理间的交互工作完成的。目前，SNMP 有 3 种：SNMP v1、SNMP v2、SNMP v3。第 1 版和第 2 版没有太大差距，但 SNMP v2 是增强版本，包含了其他协议操作。与前两种相比，SNMP v3 则包含更多安全和远程配置。为了解决不同 SNMP 版本间的不兼容问题，RFC3584 中定义了三者共存策略。

本章的重点是掌握不同版本 SNMP 的功能和特点，理解其通信的机制和应用。

习 题 3

一、选择题

1. SNMP 协议主要包括(　　)能力。

A. Get　　B. Set　　C. Proxy　　D. Trap

2. SNMP v2 既支持高度集中化的网络管理模式，又支持分布式的网络管理模式。在分布式模式下，一些系统担任管理者和代理两种角色，这种系统被称为(　　)。

A. 中间管理者　　B. 转换代理　　C. 委托代理　　D. 标准代理

3. 在通信协议操作方面，SNMP v2 增加了两个新的 PDU，它们是(　　)。

A. GetBulkResponse　　B. GetBulkRequest

C. informResponse　　D. informRequest

4. RFC2574 把安全协议分为三个模块(　　)。

A. 访问控制　　B. 认证　　C. 时间序列　　D. 加密

5. GetNextRequest PDU 与 GetRequest PDU 不同的是(　　)。

A. 相同的交换模式　　B. 原子性操作

C. 取值的对象　　D. 相同的格式

6. 下列 PDU 由代理发出的是(　　)。

A. GetRequest　　B. SetRequest

C. GetNextRequest　　D. trap

7. SNMP v3 与比前的版本相比最大的改进在于(　　)方面。

A. 效率　　B. 安全　　C. 质量　　D. 通信机制

8. WBM 有(　　)两种实现的方法，它们之间平行地发展而且互不干涉。

A. 代理方式　　B. 嵌入方式　　C. 集中方式　　D. 分布式方式

9. SNMP v2 的 GetRequest PDU 的语法和语义都与 SNMP v1 的 GetRequest PDU 相同,差别是 SNMP v2 对应答的处理(　　)。

A. 要么所有的值都返回,要么一个也不返回

B. 能够部分地对 GetRequest 操作进行应答

C. 能够全部地对 GetRequest 操作进行应答

D. 都不进行应答

二、简答题

1. 什么是陷阱引导轮询?

2. 简述 SNMP 的体系结构。

3. 什么是共同体?

4. 试比较 SNMP v2 与 SNMP v1 有什么不同。

5. 简述 SNMP v3 体系结构的组成,并说明各部分的功能。

第 4 章　远程网络监视

远程网络监视(Remote Network Monitoring,RMON)是对 SNMP 标准的重要补充,是简单网络管理向 Internet 过渡的重要步骤。RMON 扩充了管理信息库,可以提供有关 Internet 管理的主要信息,在不改变 SNMP 条件下增强了网络管理的功能。

4.1　RMON 的基本概念

4.1.1　为什么需要 RMON

1. RMON 的概念

RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由 SNMP MIB 扩展而来。RMON 中,网络监视数据包含了一组统计数据和性能指标,它们在不同的监视器(或称探测器)和控制台系统之间相互交换。结果数据可用来监控网络利用率,以用于网络规划、性能优化和协助网络错误诊断等。

当前 RMON 有两种版本:RMON v1 和 RMON v2。RMON v1 在目前使用较为广泛的网络硬件中都能发现,它定义了 9 个 MIB 组服务于基本网络监控;RMON v2 是 RMON v1 的扩展,专注于 MAC 层以上更高的流量层,它主要强调 IP 流量和应用程序层流量,允许网络管理应用程序监控所有网络层的信息包,与前者不同,后者只允许监控 MAC 及其以下层的信息包。

RMON 监视系统由两部分构成:探测器(代理或监视器)和管理者。RMON 代理在 RMON MIB 中存储网络信息,它们被直接植入网络设备(如路由器、交换机等),代理也可以是 PC 上运行的一个程序。代理只能看到流经它们的流量,所以在每个被监控的 LAN 段或 WAN 链接点都要设置 RMON 代理,管理者用 SNMP 获取 RMON 数据信息。

2. RMON 的意义

SNMP 使用嵌入到网络设施中的代理软件来收集网络通信信息和有关网络设备的统计数据。代理不断地收集统计数据,并把这些数据记录到一个 MIB 中。网络管理员通过向代理的 MIB 发出查询信号可以得到这些信息,这个过程叫轮询(polling)。

虽然 MIB 计数器将统计数据的总和记录下来了,但它无法对日常通信量进行历史分析。为了能全面地查看通信流量和变化率,管理人员就必须不断地轮询 SNMP 代理。只有这样,才能使用 SNMP 来评价网络的运行状况,揭示出通信的趋势等。但是轮询机制有如下明显的弱点:

• 没有伸缩性。在大型网络中,轮询会产生巨大的网络管理通信量,导致网络通信负

荷加重，甚至导致拥挤情况发生。

- 将收集数据的负担加在网络管理控制台上（管理进程端）。管理者所在的计算机的处理能力总是有限的，也许能轻松地收集几个网段的信息，当它们监控数十个网段时，恐怕 CPU 就无法应付。

基于上述原因，人们就提出一种高效、低成本的网络监视方案，这就是 RMON。

4.1.2 RMON 的目标

RMON 定义了远程监视的管理信息库，以及 SNMP 管理者和远程监视器之间的接口，一般 RMON 的目标只是监视子网范围内的通信，从而减少管理者和被管理者系统间的通信负担。RMON 具有下列目标：

（1）离线操作。必要时管理者可以停止对监视器的轮询，从而提高带宽利用率。即使不接受管理者查询，监视器也能不断收集子网故障、性能和配置方面信息，统计和积累数据，以便管理者查询时及时提供管理信息。另外，在网络出现异常时使其能及时向管理者报告。

（2）主动监视。如监视器有足够资源，通信负载允许，监视器可以连续地或周期地运行诊断程序，获得并记录网络性能参数。

（3）问题检测和报告。如果主动监视消耗网络资源太多，监视器也可以被动地获得网络数据。可以配置监视器，使其连续观察网络资源的消耗情况，记录随时出现的异常条件，并在出现异常时向管理者报告。

（4）提供增值数据。监视器可以分析收集到的子网数据，从而减轻管理者的计算任务。如，监视器可以分析子网的通信情况，计算出哪些主机通信最多、哪些主机出错最多等。这些数据的收集和计算由监视器来做，比由远端的管理者来做更有效。

（5）多管理者操作。一个网络可以有多个管理者，这样可以提高可靠性，或者分布地实现不同的网络管理功能。可以配置监视器使其能够并发地工作，为不同的管理者提供不同的信息。

不是每一个监视器都能实现所有目标，但 RMON 规范操作提供了实现这些目标的基础。

4.1.3 表管理原理

1. RMON 规范中的表结构

在 SNMP v1 管理框架中，对表操作的规定是很不完善的，至少行增加和行删除的操作是不明确的，这种模糊性常常是读者提问的焦点和用户抱怨的根源。RMON 规范包含一组文本约定和过程化规则，在不修改、不违反 SNMP 管理框架的前提下提供了明晰而规律的行增加和行删除操作。

在 RMON 规范中增加了两种新的数据类型，以 ASN.1 表示为：

- OwnerString∷＝DisplayString
- EntryStatus∷＝INTEGER{valid(1),createRequest(2),underCreation(3),invalid(4)}

RFC1212 规定的管理对象宏定义中，DisplayString 被定义为长 255 个字节的 OCTETSTRING 类型，这里又给了另外一个名字 OwnerString，从而赋予了新的语义。RFC1757 把这些定义叫做文本约定（textal convention），其用意是增强规范的可读性。

在每一个可读/写的 RMON 表中都有一个对象，其类型为 OwnerString，其值为表行中所有人或创建者的名字，对象名以 Owner 结尾；RMON 表中还有一对象，类型为 EntryStatus，其值表示行的状态，对象名以 Status 结尾，该对象用于行的生成、修改和删除操作。

RMON 规范中的表结构由控制表和数据表两部分组成，控制表定义数据表的结构，数据表用于存储数据。

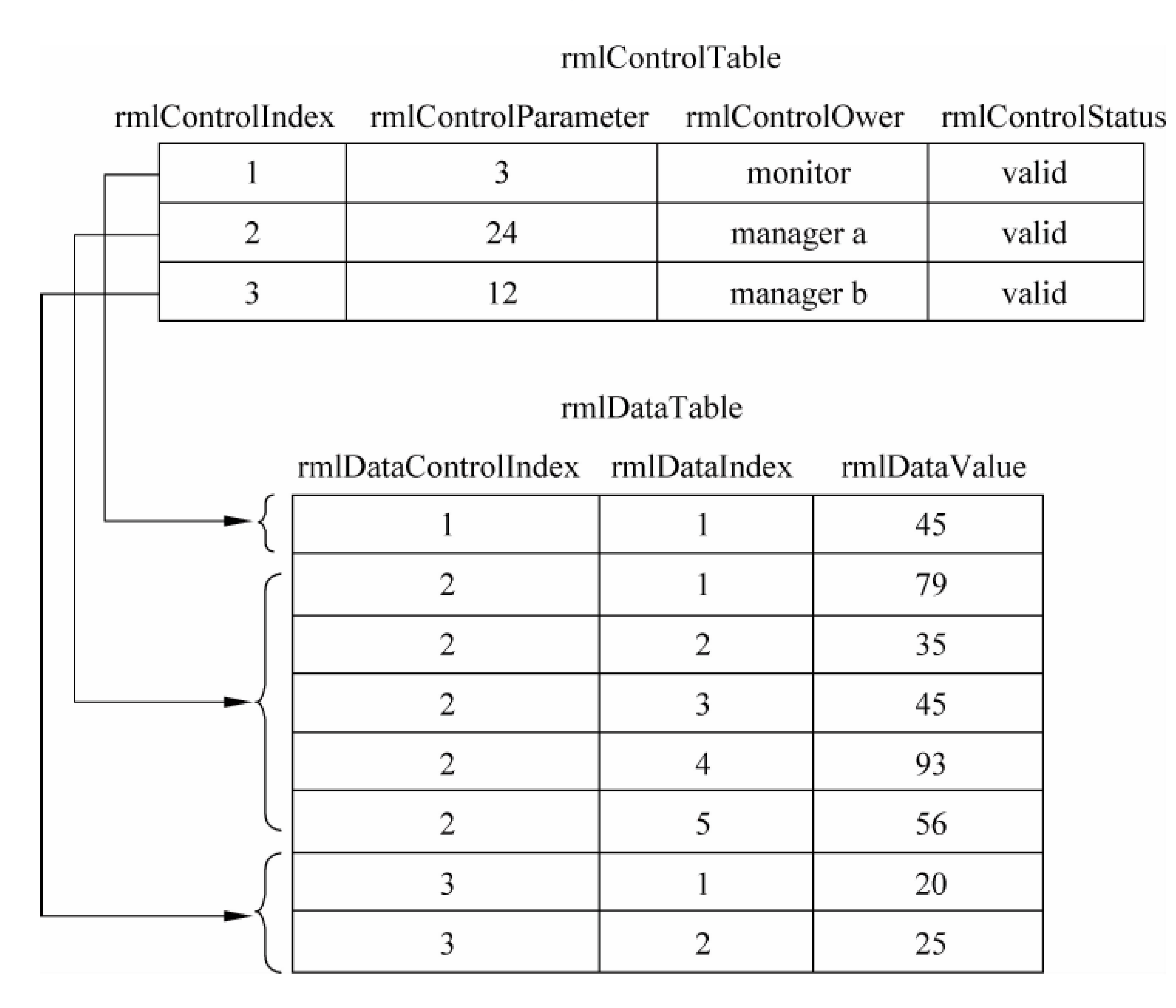
(1) 控制表

控制表包含 rmlControlIndex、rmlControlParameter、rmlControlOwner、rmlControlStatue 对象。

- rmlControlIndex：唯一地标识 rmlControlTable 中的一行，该控制行定义了 rmlDataTable 中的一个数据行集合，集合中的数据行由 rmlControlTable 的相应行控制。
- rmlControlParameter：控制参数应用于由控制行控制的所有数据行，通常有多个控制参数，而这个简单的表只有一个控制参数。
- rmlControlOwner：该控制行的所有者。
- rmlControlStatus：控制行的状态。

(2) 数据表

数据表由 rmlDataControlIndex 和 rmlDataIndex 共同索引。rmlDataControlIndex 的值与控制行的索引值 rmlControlIndex 相同，而 rmlDataIndex 的值唯一地指定了数据行集合中的某一行。图 4-1 给出了这种表的一个实例，其中控制表有 3 行，因而定义了数据表的 3 个数据行的集合。数据表的所有 rmlDataControlIndex 的值为 1 的行都由控制表的第 1 行控制，数据表中所有 rmlDataControlIndex 值为 2 的行都由控制表的第 2 行控制，数据表中所有 rmlDataControlIndex 值为 3 的行都由控制表的第 3 行控制。控制表中的第一行的所有者为 monitor，按照约定这是指代理本身。



rmlControlTable

rmlControlIndex	rmlControlParameter	rmlControlOwer	rmlControlStatus
1	3	monitor	valid
2	24	manager a	valid
3	12	manager b	valid

rmlDataTable

rmlDataControlIndex	rmlDataIndex	rmlDataValue
1	1	45
2	1	79
2	2	35
2	3	45
2	4	93
2	5	56
3	1	20
3	2	25

图 4-1　RMON 表的实例

2. 增加行

管理者用 set 命令在 RMON 表中增加行，并遵循下列规则：

(1) 管理者用 SetRequest 生成一个新行，如果新行的索引值与其他行的索引值不冲突，则代理产生一个新行，其状态值为 createRequest(2)。

(2) 新行产生后，由代理把状态对象的值置为 underCreation(3)。对于管理者没有设置新值的列对象，代理可以置为默认值，或者让新行维持这种不完整、不一致的状态。

(3) 新行的状态值保持为 underCreation(3)，直到管理者产生了所要生成的新行。这时由管理者置每一新行状态的对象的值为 valid(1)。

(4) 如果管理者要生成的新行已经存在，则返回一个错误值。

以上算法的效果是，在多个管理者请求产生同一概念行时，仅最先到达的请求成功，其他请求失败。另外，管理者也可以把一个已存在的行的状态对象的值由 invalid 改写为 valid，恢复旧行的作用，这等于产生了一个新行。

3. 删除行

只有行的所有者才能发出 SetRequestPDU，把行状态值置为 invalid(4)，这样就删除了行。这种删除是否为物理删除，取决于具体的实现。

4. 修改行

首先置行状态对象的值为 invalid(4)，然后用 SetRequestPDU 改变行中其他对象的值。

4.1.4 多管理者访问

RMON 监视器应允许多个管理者并发地访问，当多个管理者访问时可能出现以下问题：

(1) 多个管理者对资源的并发访问可能超过监视器的能力。

(2) 一个管理者可能长时间占用监视器资源，使得其他管理者得不到访问。

(3) 占用监视器资源的管理者可能出现崩溃，而没有释放资源。

RMON 控制表中列对象 Owner 规定了表的所属关系，所属关系有以下用法，可以解决多个管理者并发地访问的问题：

(1) 管理者能认得自己所属的资源，也知道自己不再需要的资源。

(2) 网络管理员可以知道管理者占有的资源，并决定是否释放这些资源。

(3) 一个被授权的网络管理员可以自主决定是否释放其他网络管理员的资源。

(4) 如果管理者重新启动，它应该首先释放不再使用的资源。

RMON 规范建议，所属标志应包括 IP 地址、管理者名、网络管理员的名字、地点和电话号码等，所属标志不能作为口令或访问控制机制使用。在 SNMP 管理框架中唯一的访问控制机制是 SNMP 视阈和团体名。如果一个可读/写的 RMON 控制表出现在某些管理者的视阈中，则这些管理者都可以进行读/写访问，但是控制表行只能由其所有者改变或删除，其他管理者只能进行读访问。这些限制的实施已超出了 SNMP 和 RMON 的范围。

为了提供共享的功能，监视器通常配置一定的默认功能。定义这些功能的控制行的所有者是监视器，所属标志的字符串以监视器名打头，管理者只能以读方式利用这些功能。

4.2 RMON 的管理信息库

RMON 规范定义了 RMON 管理信息库(RMON MIB),它是 MIB-2 下面的 16 个子树。如表 4-1 所示,RMON MIB 分为 10 组,存储在每一组中的信息都是监视器从一个或几个子网中统计和收集的数据。这 10 个功能组都是任选的,但实现时有下列连带关系:

- 实现告警组时必须实现事件组。
- 实现 HostTopN 台主机组时必须实现主机组。
- 实现捕获组时必须实现过滤组。

表 4-1 RMON v1 MIB 功能组

功能组名称	功　能	元　素
统计量 statistics(1)	包含一个设备上的每个监视接口的统计数据	数据包丢弃、数据包发送、广播数据包、CRC 错误、大小块、冲突以及计数器的数据包。范围为 64～128、128～256、256～512、512～1024 以及 1024～1518 字节
历史 history(2)	周期性地从统计组中获取统计采样信息	取样周期、样品数目和项目,提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据
告警 alarm(3)	允许管理员针对任何 RMON 代理记录的计数器变量或整型变量设置采样间隔和报警阈值	告警类型、间隔、阈值上限、阈值下限
主机 host(4)	包含网络上发现的与每个主机相关的统计值	主机地址、数据包、接收字节、传输字节、广播传送等
HostTopN(5)	包括了在统计列表中排名大于主机表中设定的某个参数的主机统计值	统计值、主机、周期的开始和结束、速率基值、持续时间
矩阵 matrix(6)	记录关于子网上两个主机之间流量的信息,该信息以矩阵形式存储起来	源地址和目的地址对、数据包、字节和每一对的错误
过滤器 filter(7)	允许监视器监听与一过滤器相匹配的数据包	字节过滤器类型、过滤器表达式等
捕获包 capture(9)	数据包在流过一个信道之后被捕获	捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计
事件 event(9)	控制在此处事件的产生和报告	事件类型、描述、事件最后一个发送的时间
令牌环 tokenRing(10)	支持令牌环	不常使用

4.3 RMON v2 管理信息库

4.3.1 RMON v2 MIB 的组成

RMON v2 是 RMON v1 的扩展,可以监视 OSI 第 3～7 层的通信,能够对数据链路层以上的分组进行译码。这使得监视器可以管理网络层协议,因而可以了解分组的源地址和

目的地址，知道路由器负载的来源，使得监视的范围扩大到局域网以外。监视器也可以监视应用层协议，记录主机应用活动的数据，并可以显示各种应用活动的图表，这对网络管理来说具有非常重要的意义。RMON v2 在 RMON v1 MIB 的基础上增加了 9 个新功能组，这些组的功能如表 4-2 所示。

表 4-2　RMON v2 MIB 新增功能组

RMON v2 MIB 功能组	功　　能
协议目录 protocolDir(11)	协议目录是一种简单的便于共同建立应用程序、实现 RMON 代理的途径。这对于应用程序和代理出自不同的提供商的情况尤其重要
协议分布 protocolDist(12)	提供每个协议产生的通信统计数据，如发送了多少分组，多少字节等
地址映像 addressMap(13)	MAC 层的地址与网络层的地址之间的转换使得读和记忆变得容易。地址转换不仅为网络管理者提供了帮助，而且它支持 SNMP 管理平台并引入了改进的拓扑布局转换
网络层主机 nHost(14)	网络层主机(IP 层)统计值
网络层矩阵表 nMatrix(15)	在两个地址之间存储并重新获取网络层主机(IP 层)统计值
应用层主机 alHost(16)	应用层主机统计值
应用层矩阵表 alMatrix(17)	在两个地址之间存储并重新获取应用层主机(IP 层)统计值
用户历史 usrHistory(18)	这一特性使网络管理员能够配置系统中的任何历史记录，例如在指定文件服务器或路由器对路由器的连接上的特殊历史
监视器配置 probeConfig(19)	RMON v2 的这一特性使某些提供商的 RMON 应用程序能够配置其他提供商的 RMON 监视器

4.3.2　RMON v2 增加的功能

RMON v2 引入了两种与对象索引有关的新功能：外部对象索引，时间过滤器索引，增强了 RMON v2 的能力和灵活性。

1. 外部对象索引

在 SNMP v1 的 SMI 宏定义中，没有说明索引对象是否必须是被索引表的列对象，在 SNMP v2 的 SMI 中已经明确指出可以使用不是概念表成员的对象作为索引项。在这种情况下，必须在概念行的 DESCRIPTION 子句中给出文字解释，说明如何使用这样的外部对象唯一地标识概念行实例。

采用了这种新的表结构后，应经常使用外部对象索引数据表，以便把数据表与对应的控制表结合起来。在 rm1 表中，数据表有两个索引对象，第一个索引对象 rm1DataControlIndex 只是重复了控制表的索引对象。在 rm2 的数据表中，这个索引对象没有了，只剩下了唯一的索引对象 rm2DataIndex。但是在数据表的概念行定义中说明了两个索引 rm2ControlIndex 和 rm2DataIndex，同时在 rm2DataIndex 的描述子句中说明了索引的结构。

例如要检索第三行定义的第 50 个数据值，则对象实例的标识为 rm2DataValue. 3. 50，比 RMON v1 的数据表少一个作为索引的列对象。此外，SNMP v2 的一个文本约定为：RMON v2 状态对象的类型用 RowStatus 表示，而不是 EntryStatus。

2. 时间过滤器索引

网络管理应用需要周期地轮询监视器，以便得到被管理对象的最新状态信息。为了提

高效率，使用时间过滤器索引，使监视器每次只返回那些自上次查询以来改变了的值。SNMP v1 和 SNMP v2 中都没有直接解决这个问题的方法。然而 RMON v2 的设计者却给出了一种新颖的方法，在 MIB 的定义中实现了这个功能，这就是用时间过滤器进行索引。

RMON v2 引入了一个新的文本约定：类型为 TimeFilter 的对象专门用于表索引，其类型也就是 TimeTicks。这个索引的用途是使得管理者可以从监视器取得自从某个时间以来改变过的变量，这里的时间由类型为 TimeFilter 的对象表示。

4.4 RMON v2 的应用

4.4.1 协议的标识

任何一个网络都可能运行许多不同的协议，有些协议是标准的，有些是专用于某种特定产品的。一个网络运行的各个协议之间还有复杂的关系，如可能同时运行多个网络层协议（IP、IPX），一个 IP 有多个数据链路层协议的支持，而 TCP 和 UDP 同时运行于 IP 之上等。在远程网络监视中必须能够识别各种类型的网络协议，表示协议之间的关系，RMON v2 提供了表示协议类型和协议关系信息的标准方法。

RMON v2 用协议标识符和协议参数共同表示一个协议以及该协议与其他协议之间的关系。协议标识符是由字节串组成的分层的树结构，类似于 MIB 对象组成的树。RMON v2 赋予每一个协议层 32 位的字节串，编码为 4 个十进制数，表示为[a. b. c. e]的形式，这是协议标识符树的节点。如，各种数据链路层协议被赋予下面的字节串：

```
ether2        =1[0.0.0.1]
llc           =2[0.0.0.2]
snap          =3[0.0.0.3]
vsnap         =4[0.0.0.4]
wgAssigned    =5[0.0.0.5]
anylink       = [1.0.a.b]
```

最后的 anylink 是一个通配符，可指任何链路层协议。有时监视器可以监视所有的 IP 数据报，而不知它是包装在什么链路层协议中，这时可以用 anylink 说明 IP 下面的链路层协议。

链路层协议字节串是协议标识符树的根，下面每个直接相连的节点是链路层协议直接支持的上层协议，或者说是包装在数据链路帧中的协议（通常情况下是网络层协议）。整个协议标识符树就是这样逐级构造的，如图 4-2 所示，这时表示的是以太网协议直接支持 IP，UDP 运行于 IP 之上，最后，SNMP 报文封装在 UDP 数据报中传送，用文字表示就是 ether2. ip. udp. snmp。

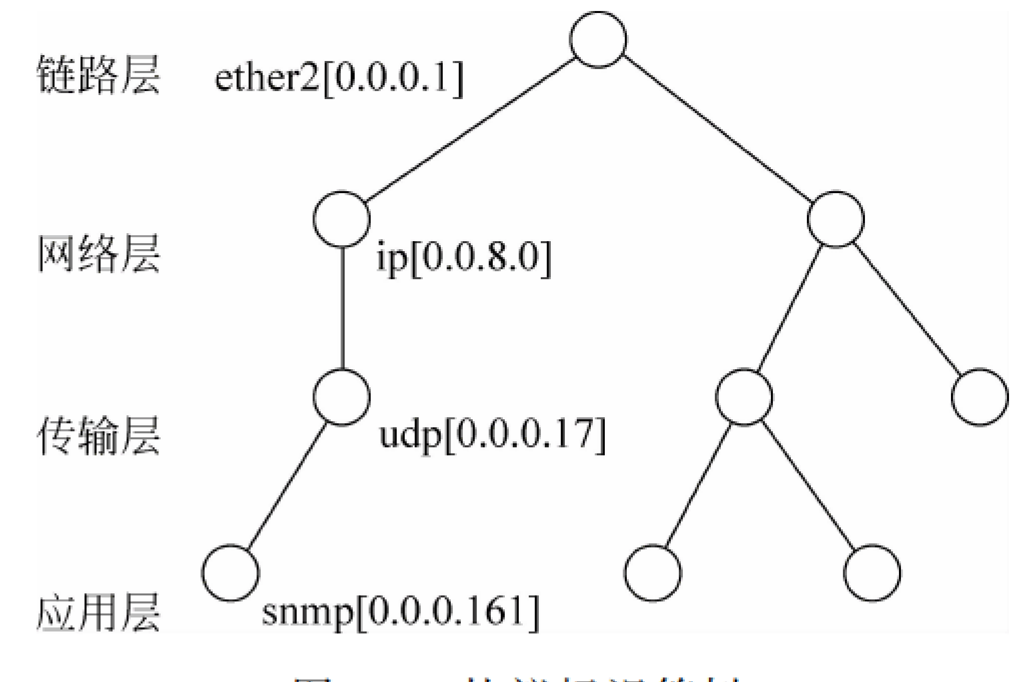


图 4-2 协议标识符树

RMON v2 的协议标识符的格式如图 4-3 所示。开头有一个字节的长度计数段 cnt，后续为各层协议的子标识符字段。每层协议的子标识符都与上述链路层协议字节串相似，是 32 位，编码为 4 个十进制数。从图 4-2 可以看到赋予以

太 2(ether2)协议的字节串是[0.0.0.1],以太网之上的协议字节串形式为[0.0.a.b],其中 a 和 b 是以太 2 协议 MAC 帧中的类型字段的 16 位二进制,这 16 位数用来表示 2 型以太网协议支持的上层(网络层)协议,以太 2 规范为 IP 分配的字节串是[0.0.8.0]。与此类似,在 IP 头中的 16 位协议号表示 IP 支持上层协议,IP 标准为 UDP(传输层)分配的编号是 17。UDP 为 SNMP(应用层)分配的端口号为 161。这样 4 层协议的字节串级联起来,前面加上 16 表示长度,就形成了完整的 SNMP 协议标识符:

16.0.0.0.1.0.0.8.0.0.0.0.17.0.0.0.161

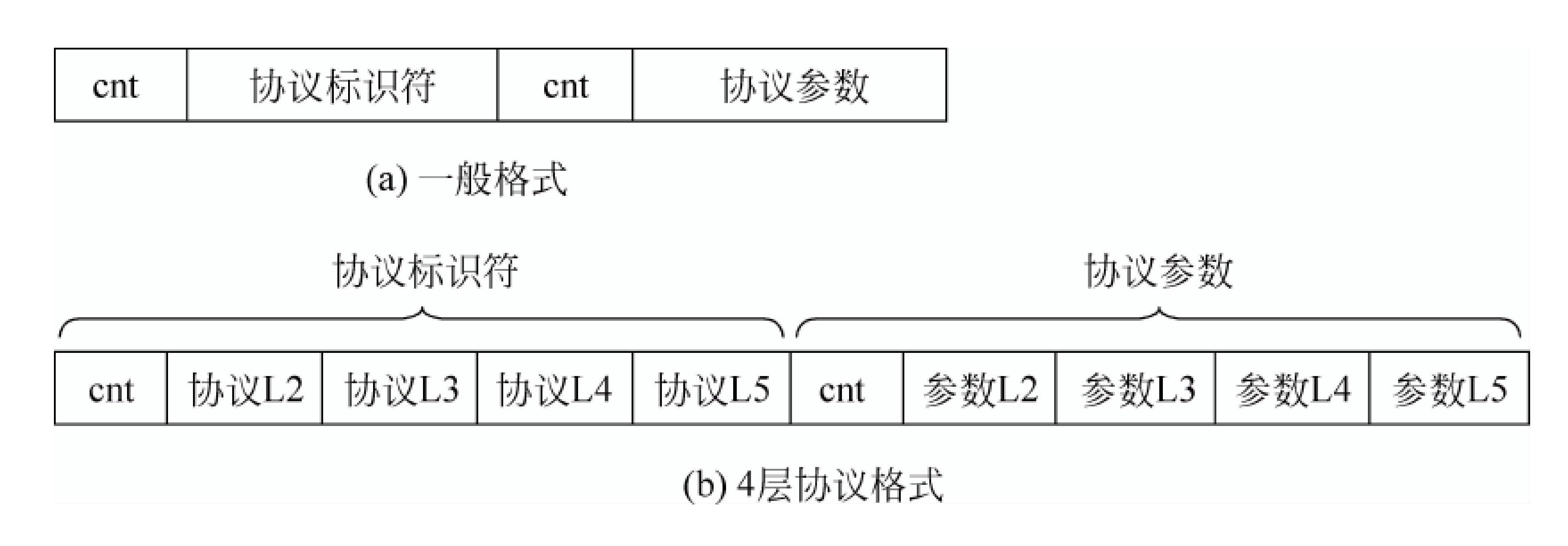


图 4-3　协议标识符和协议参数的格式

应该强调的是:对监视器能解释的每个协议都必须有一个协议标识符。假如有个监视器可以识别以太 2 帧 IP 和 UDP 数据报,以及 SNMP 报文,则 RMON v2 MIB 中必须记录以下 4 个协议标识符:

ether2(4.0.0.0.1)
ether2.ip(8.0.0.0.1.0.0.8.0)
ether2.ip.udp(12.0.0.0.1.0.0.8.0.0.0.0.17)
ether2.ip.udp.snmp(16.0.0.0.1.0.0.8.0.0.0.0.17.0.0.0.161)

从图 4-3 中可以看出协议参数的格式,长度计数字段 cnt 后跟各层协议的参数。参数的每一个比特定义了一种能力。例如,最低两比特的含义如下:

- 比特 0——表示允许上层协议 UDP 分段。如果上层报文可以分成若干 IP 数据报传送,则 IP 层的参数比特 0 为 1。
- 比特 1——表示可以为上层协议指定端口号。如 TFTP 协议,其专用端口号是 69。如果上层用户进程向端口 69 请求连接,TFTP 进程响应用户请求,派生出一个临时进程,并为其分配临时端口号,返回用户进程,用户就可以用 TFTP 传送文件了。

现在可以把上例中的协议标识符加上协议参数。如果表示 IP 之上的协议 UDP 可以分段传送,则协议标识符和协议参数串如下:

16.0.0.0.1.0.0.8.0.0.0.0.17.0.0.0.161.4.0.1.0.0

4.4.2　协议目录表

RMON v2 的协议目录表的结构如图 4-4 所示,其中的协议标识符 protocolDirID(1)和协议参数 protocolDirParameters(2)作为表项的索引,另外还为每个表项指定了一个唯一的

索引 protocolDirLocalIndex(3),可由 RMON v2 的其他组引用该表项,其他变量的功能为:

- protocolDirDesc(4):关于该协议的文字描述。
- protocolDirType(5):协议类型是可扩展的,如果表中生成一个新项,则所表示的是该协议的孩子。协议类型是具有地址识别能力的,如果监视器可以区别源地址和目标地址,则分别对源和目标计数。
- protocolDirAddressMapConfig(6):表示协议是否支持(网络层对数据链路层)地址映像。
- protocolDirHostConfig(7):与网络层和应用层主机表有关。
- protocolDirMatrixConfig(8):与网络层和应用层矩阵表有关。
- protocolDirOwner(9):目录的拥有者。
- protocolDirStatus(10):目录的状态。

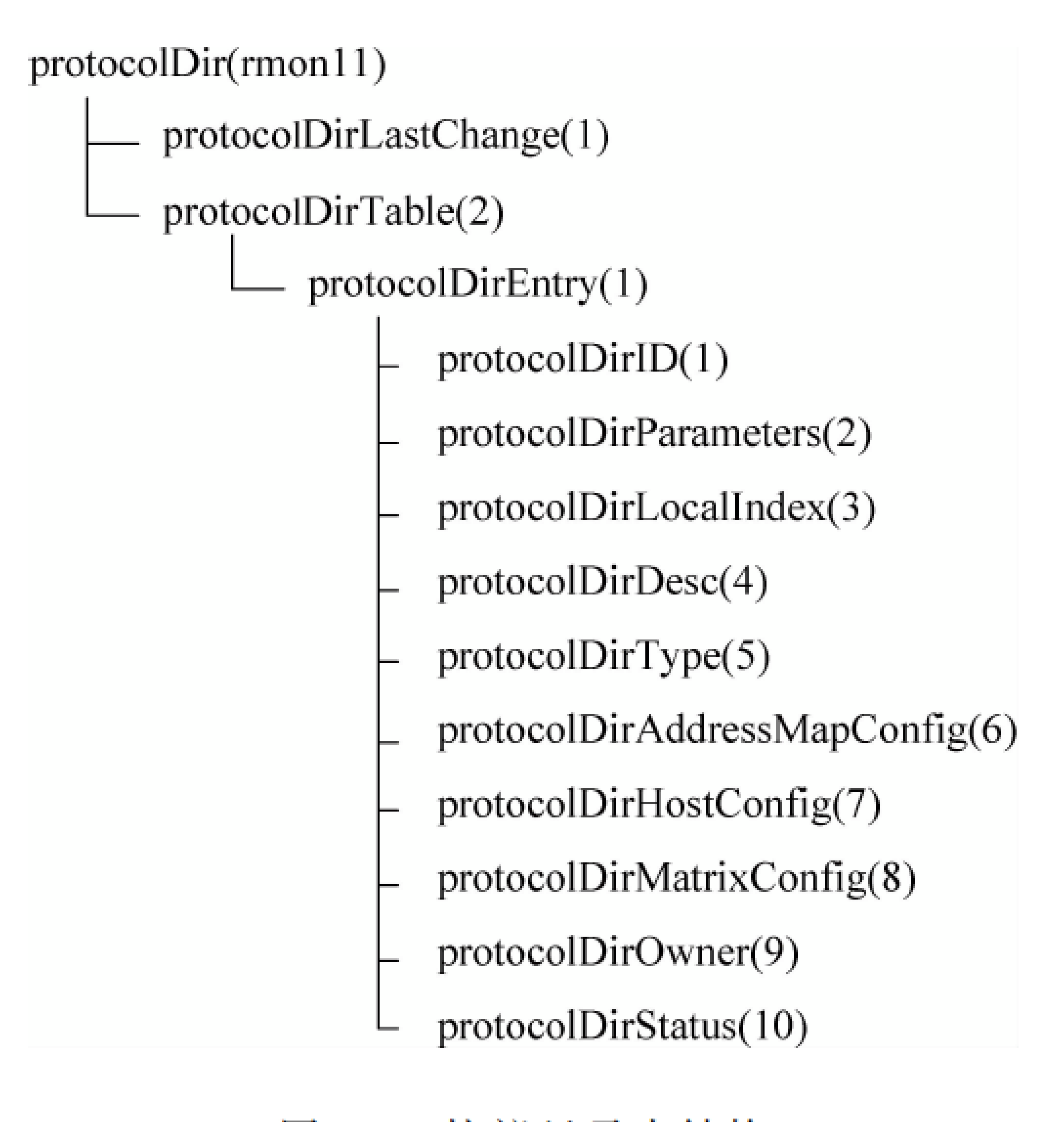


图 4-4 协议目录表结构

4.4.3 用户定义的数据收集机制

关于历史数据收集,在 RMON v1 中是预先定义的,在 RMON v2 中可以由用户自己定义。历史收集组规定了定义历史数据的方法。

历史收集组由 3 级表组成,第一级是控制表 usrHistoryControlTable,这个表说明了一种采样功能的细节(采样的对象数、采样区间数和采样区间长度等),它的一行定义了下一级的一个表。第二级是用户历史对象表 usrHistoryObjectTable,它也是一个控制表,说明采样的变量和采样类型,该表的行数等于上一级表定义的采样对象数。第三级表 usrHistoryTable 才是历史数据表,该表由第二级表的一行控制,记录着各个采样变量的值和状态,以及采样间隔的起止时间,用户历史收集组如图 4-5 所示。

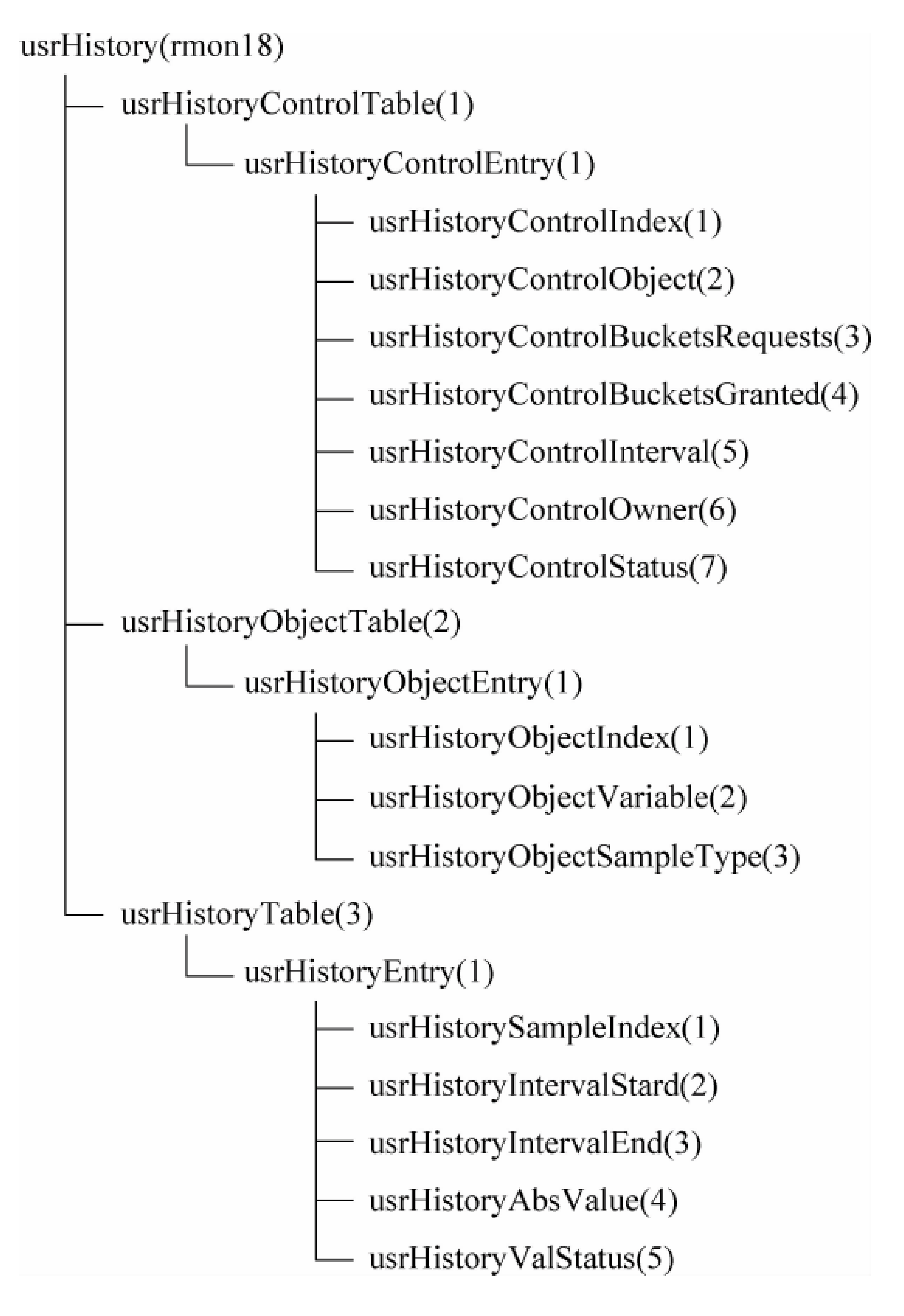


图 4-5　历史收集组

4.4.4　监视器的标准配置法

为了增强管理者和监视器之间的互操作性，RMON v2 在监视器配置组中定义了远程配置监视器的标准化方法。这个组由一些标量对象和 4 个表组成，这些标量对象如下：

- probeCapabilities——说明支持哪些 RMON 组。
- probeSoftwareRev——监视器的软件版本。
- probeHardwareRev——监视器的硬件版本。
- probeDataTime——监视器的日期和时间。
- probeResetControl——可以取不同的值，表示运行、热启动或冷启动等。
- probeDownloadFile——自举配置文件。
- probeDownloadTFTPServer——自举配置文件所在的 TFTP 服务器地址。
- probeDownloadAction——若取值 imageValid（1），则继续运行；若取值 downloadToPROM(2)或 downloadRAM(3)，则重启动，装入另外一个应用程序。
- probeDownloadStatus——表示不同的运行状态。

监视器配置组中的 4 个表是串行配置表、网络配置表、陷入定义表和串行连接表。串行配置表(serialConfigTable)用于定义监视器的串行接口，它包含下列变量：

- serialMode——连接模式可以是直接连接或通过调制解调器连接。

- serialProtocol——数据链路层协议可以是 SLIP 或其他协议。
- serialTimeout——终止连接之前等待的秒数。
- serialModemInitiString——用于初始化 Modem 的控制字符串。
- serialModemHangUpString——断开 Modem 连接的控制字符串。
- serialModemConnectResp——描述 Modem 响应代码和数据速率的 ASCII 串。
- serialModemNoconnectResp——由 Modem 产生的报告连接失效的 ASCII 串。
- serialDialoutTimeout——拨出等待时间。
- serialStatus——描述串行配置表当前状态的字符串。

网络配置表(netConfigTable)用于定义监视器的网络接口,它包含下列变量:

- netConfigIpAddress——接口的 IP 地址。
- netConfigSubnetMask——子网掩码。
- netDefaultGateway——默认网关的 IP 地址。

陷入定义表(trapDestTable)定义了陷入的目标地址等有关信息,它包含的变量如下:

- trapDestIndex——行的索引。
- trapDestCommunity——接收陷入的团体名。
- trapDestProtocol——传入陷入报文的协议。
- trapDestAddress——接收陷入站的地址。
- trapDestOwner——陷入目标的拥有者。
- trapDestStatus——陷入目标的当前状态。

串行连接表(serialConnectionTable)存储与管理者建立 SLIP 连接需要的参数,其中有下列变量:

- serialConnectIndex——行索引。
- serialConnectDestIpAddress——SLIP 连接的 IP 地址。
- serialConnectType——可分为 direct(1)、modem(2)、switch(3)、modemSwitch(4)共 4 种类型。
- serialConnectDialString——控制建立 Modem 连接的字符串。
- serialConnectSwitchConnectSeq——控制建立数据交换连接的字符串。
- serialConnectSwitchDisconnectSeq——控制终止数据交换连接的字符串。
- serialConnectSwitchResetSeq——使数据交换连接复位的字符串。
- serialConnectOwner——描述串行连接表拥有者的字符串。
- serialConnectStatus——描述串行连接表当前状态的字符串。

4.5 本章小结

本章首先介绍了 RMON 的基本概念,然后分别介绍了 RMON v1 和 RMON v2 的 MIB,最后介绍了 RMON v2 的应用。需要掌握 RMON 的概念、作用和功能,以及 RMON 中典型操作的原理。

RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题,用于监视整个网络通信情况。RMON 是对 SNMP 的补充,扩充了 SNMP 的 MIB-2,基于

RMON 协议的设备称为网络监视器或网络分析器、探测器等。RMON 提供了一种高效、低成本的网络监视方案。

习　题　4

一、选择题

1. 在 RMON 规范中增加了两种新的数据类型，它们分别是(　　)。

A. createRequest　　B. underCreation

C. EntryStatus　　D. OwnerString

2. RMON v1 监视 OSI 第 1、2 层的通信，而 RMON v2 监视 OSI(　　)的通信。

A. 第 3～7 层　　B. 第 7 层

C. 第 4～7 层　　D. 第 3～4 层

3. RMON v2 在监视器配置组中定义了远程配置监视器的标准化方法。这个组由一些标量对象和 4 个表组成，下列选项中不是其中的表的是(　　)。

A. 网络配置表　　B. 串行配置表　　C. 陷入定义表　　D. 并行配置表

4. RMON 是对(　　)标准的重要补充。

A. SNMP　　B. SMTP　　C. UDP　　D. ICMP

5. RMON v2 监视器配置组中，存储与管理者建立 SLIP 连接参数的是(　　)。

A. 串行配置表　　B. 网络配置表　　C. 陷入定义表　　D. 串行连接表

6. 通常用于监视整个网络(　　)情况的设备称为网络监视器或网络分析器、探测器等。

A. 通信　　B. 差错率　　C. 传输率　　D. 管理

二、简答题

1. 什么是 RMON？为什么需要 RMON？
2. 远程网络监视的目标是什么？
3. RMON 是如何解决多个管理者并发访问问题的？
4. RMON v2 增加了哪些功能？
5. RMON v2 如何表示协议间的关系？

第5章 网络设备管理

网络是由网络设备搭建起来的,网络设备的稳定性直接决定了网络的性能,影响业务的开展。而网络设备的正确配置是应用的前提,网络设备的有效管理是应用效率和效益的保证。本章将主要介绍基于 Windows Server 2003 服务的配置与管理,以及交换机、路由器等主要网络设备的配置与管理。

5.1 服务器管理

5.1.1 Web 服务器管理

1. 域控制器的配置

Windows Server 2003 中的域是网络中的一个逻辑单位,分为根域和子域,每个域由一个或多个域控制器管理。域控制器是域中的管理计算机,包含了由域的账户、密码、属于这个域的计算机等信息构成的数据库,负责对整个 Windows 域以及域中的所有计算机进行管理。

在 Windows Server 2003 中,域中所有的域控制器都是平等的关系。在网络中创建第一个域控制器的同时,也创建了第一个域、第一个域林和第一个站点,并安装了 Active Directory,域控制器的配置过程如下:

(1) 依次单击“开始”→“程序”→“管理工具”→“配置您的服务器向导”,然后单击“下一步”按钮。

(2) 在出现的对话框的“配置选项”中选中“第一台服务器的典型配置”单选按钮,然后单击“下一步”按钮。

(3) 在“Active Directory 域名” 对话框中输入标准格式的域,如图 5-1 所示。

(4) 配置“DNS 转发查询”,检查“选择总结”,无误后单击“下一步”按钮,即完成域控制器的配置。

2. IIS 的配置

Web 服务器的建立需要 IIS 组件的支撑,如果该组件没有安装,则按如下步骤添加:

在“控制面板”中选择“添加/删除程序”→“添加/删除组件”,在打开的对话框中选择“应用程序服务器”;单击“详细信息”按钮,选中“Internet 信息服务(IIS)”,如图 5-2 所示;然后单击“确定”按钮完成 IIS 的安装。

3. 网站的建立

(1) 将要发布的网站的内容(本例为主页 homepage.txt)复制到一个指定的目录下(默认为 C:\Inetpub\wwwroot,建议更改)。

(2) 打开如图 5-3 所示的 IIS 管理器窗口。

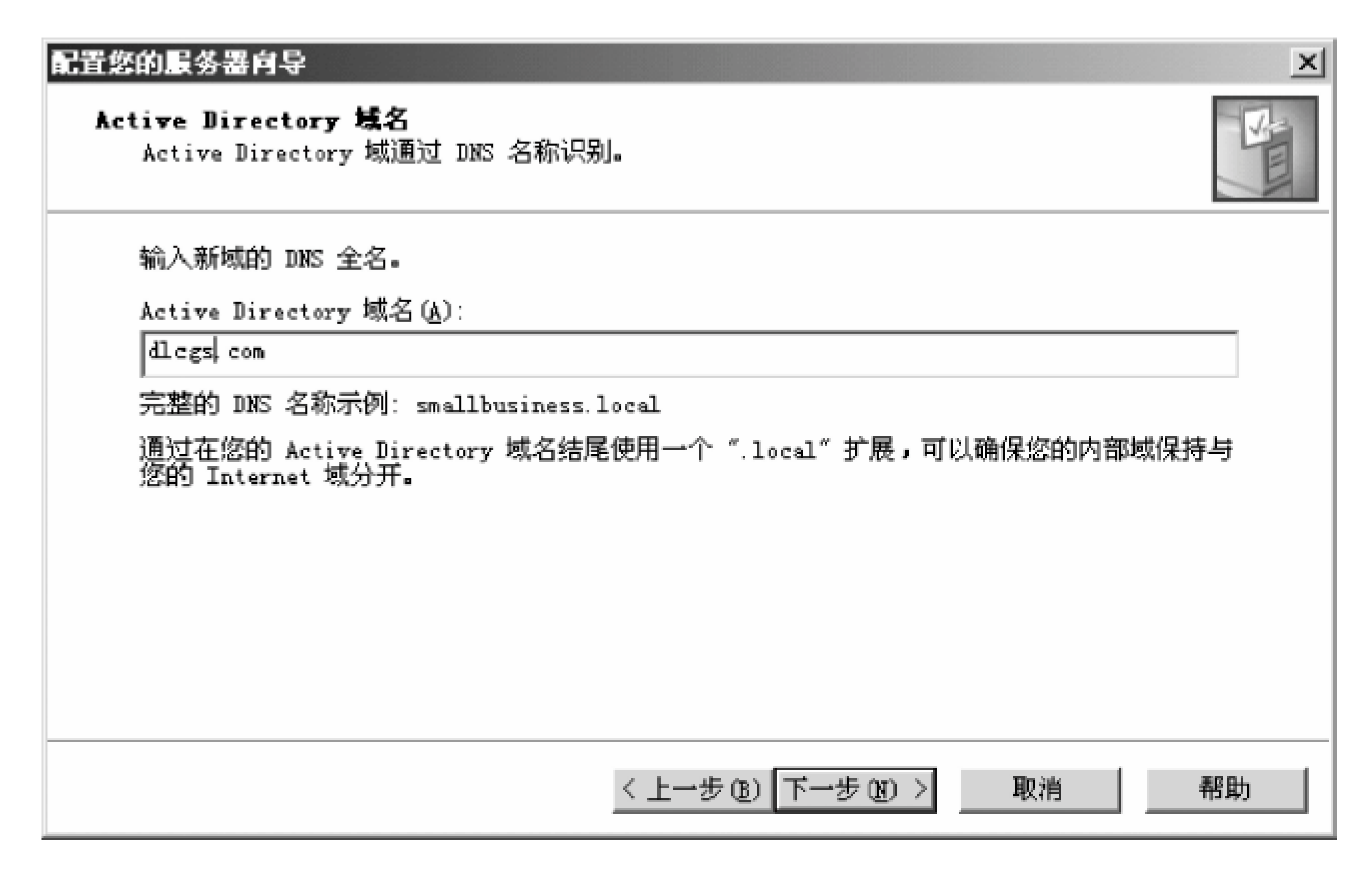


图 5-1　输入域名

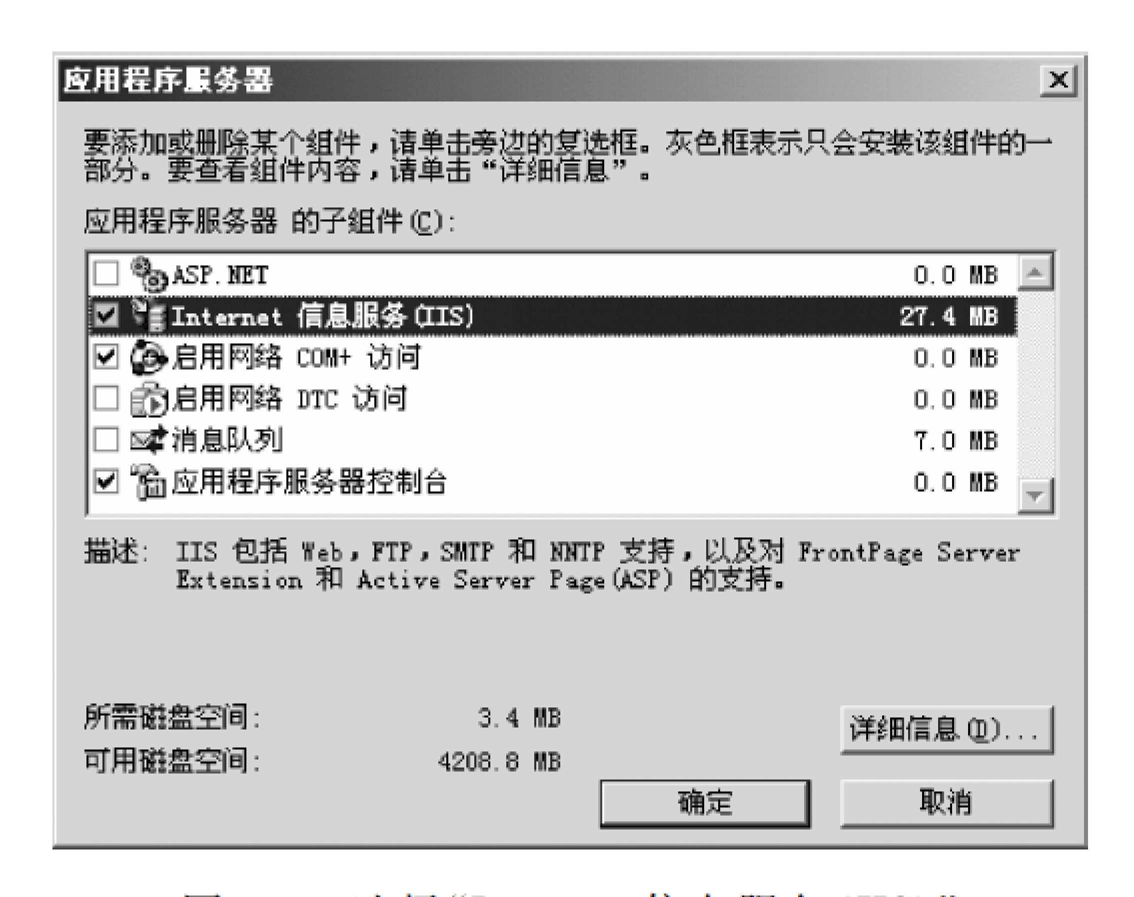


图 5-2　选择"Internet 信息服务(IIS)"

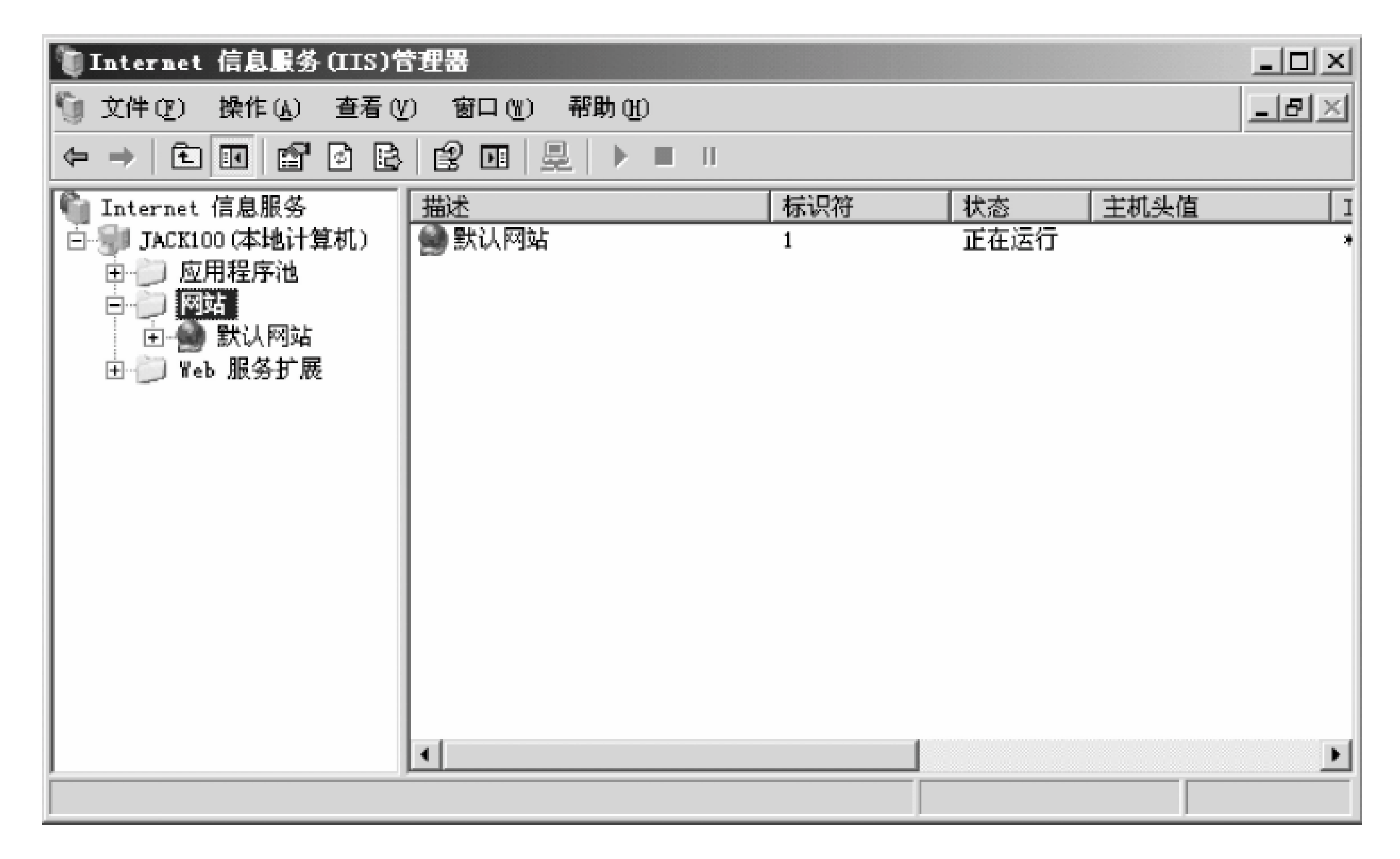


图 5-3　IIS 管理器窗口

(3) 在"网站"上单击鼠标右键，在出现的快捷菜单中选择"新建"→"网站"命令，打开"网站创建向导"对话框；单击"下一步"按钮后输入网站描述的内容。

(4) 继续单击"下一步"按钮，打开如图 5-4 所示的对话框，在"网站 IP 地址"下拉列表框

中选择该网站的 IP 地址；在“网站 TCP 端口”文本框中输入端口号(默认值为 80)；“此网站的主机头”可以根据实际情况填写。

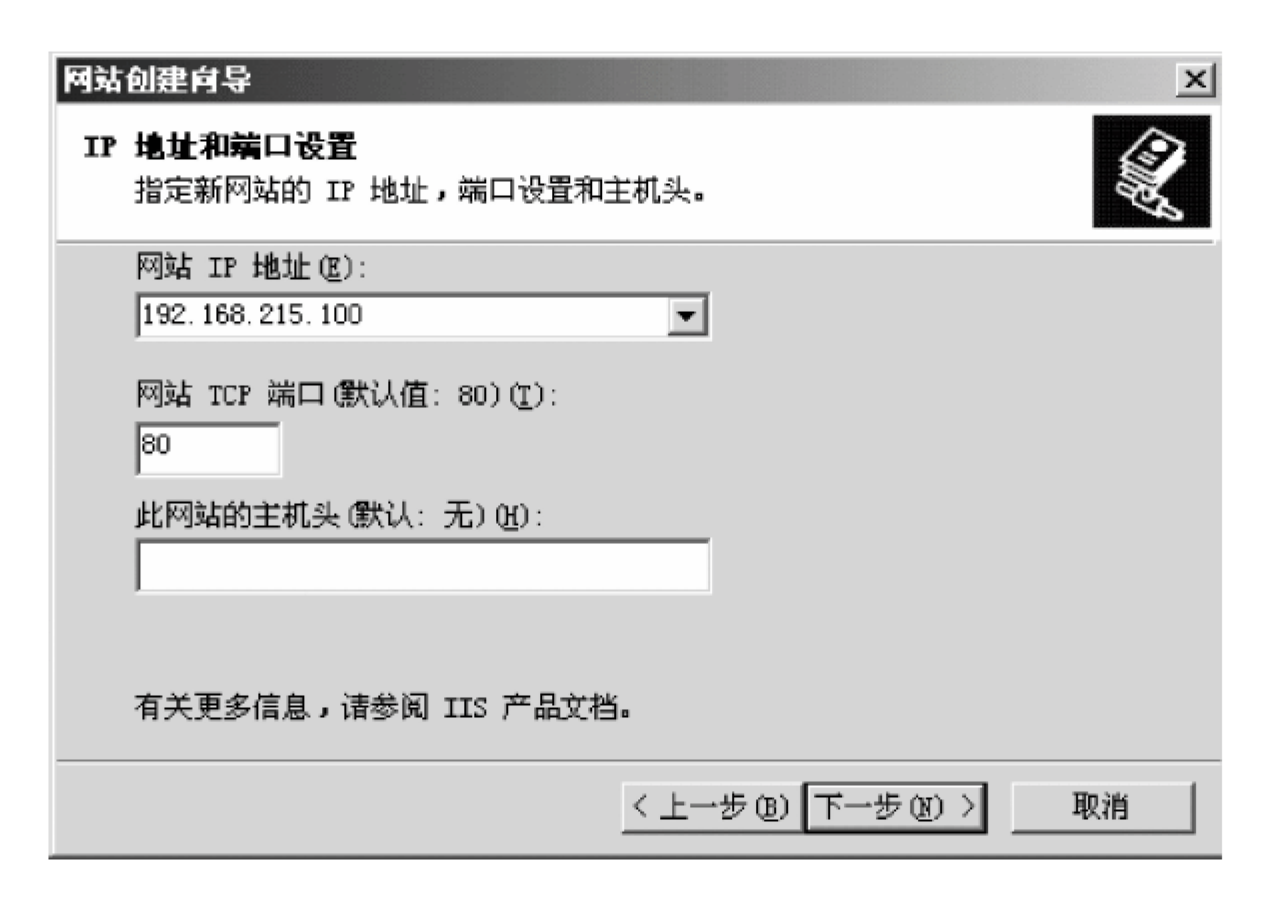


图 5-4 “IP 地址和端口设置”对话框

(5) 单击“下一步”按钮，在打开的对话框的“路径”文本框中输入或通过“浏览”按钮添加要发布网站的路径，并选中“允许匿名访问网站”复选框。

(6) 单击“下一步”按钮，在出现的对话框中，对该网站的访问权限进行适当的设置。然后单击“下一步”按钮，完成网站的创建。

(7) 在已经建立的网站上单击鼠标右键，在出现的快捷菜单中选择“属性”，然后在出现的对话框中打开“文档”选项卡，选择“启用默认内容文档”复选框，这时发现系统默认的文档中并没有用户自己事先建立的主页 homepage.txt。

(8) 单击“添加”按钮，在出现的对话框中，输入要添加的文档 homepage.txt。

(9) 单击“确定”按钮，这时发现新添加的文档会显示在默认文档的最后一行。由于 Web 服务器响应客户端的请求时会在默认文档的最前面逐次尝试，为了加快该网站的响应速度，最好把 homepage.txt 文档移动到最前面，如图 5-5 所示。

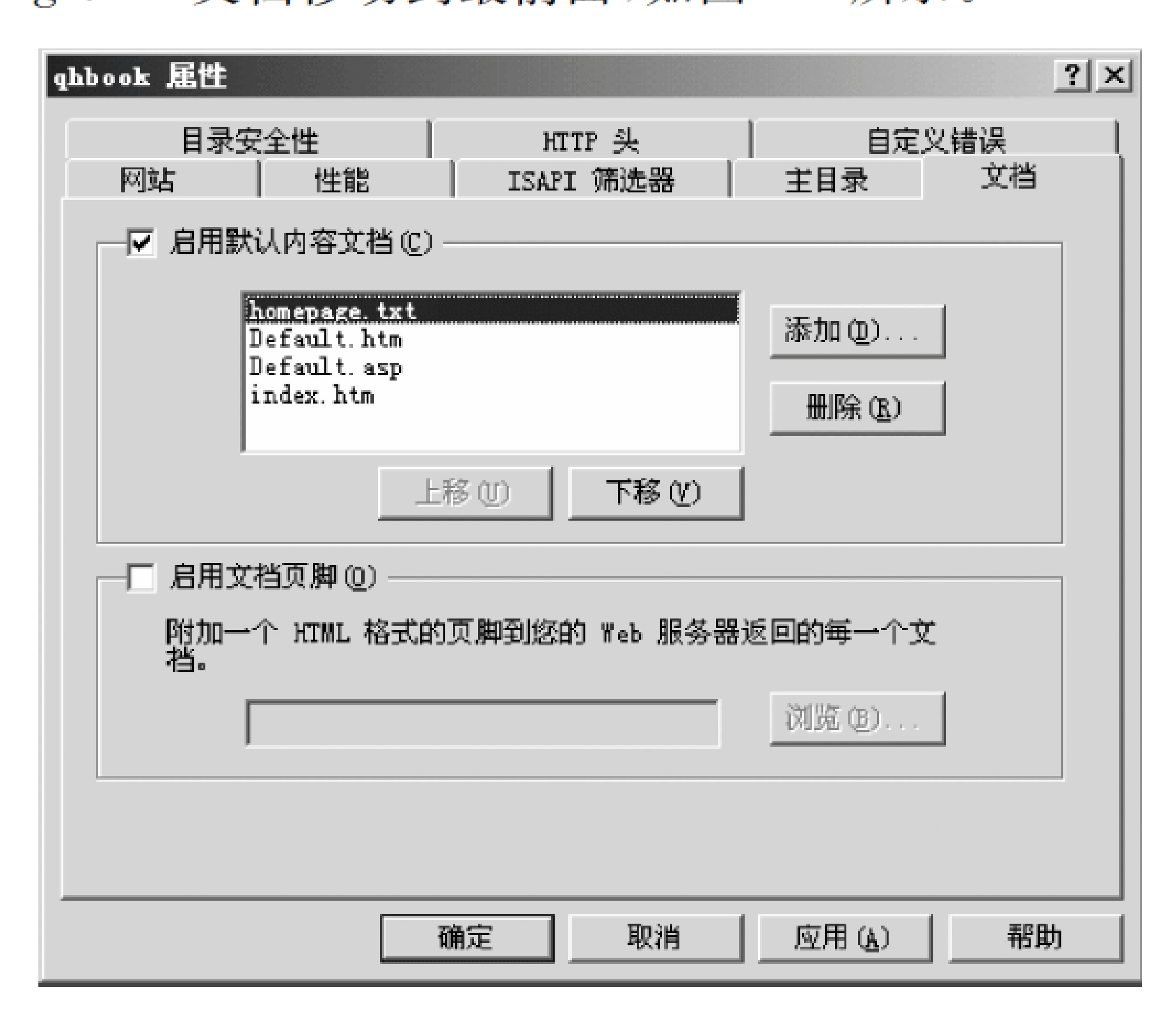


图 5-5 “文档”选项卡

(10) 单击"确定"按钮，完成网站的配置。在客户机的 IE 浏览器中输入 http://192.168.215.100 后，即可打开该网站的主页，如图 5-6 所示。

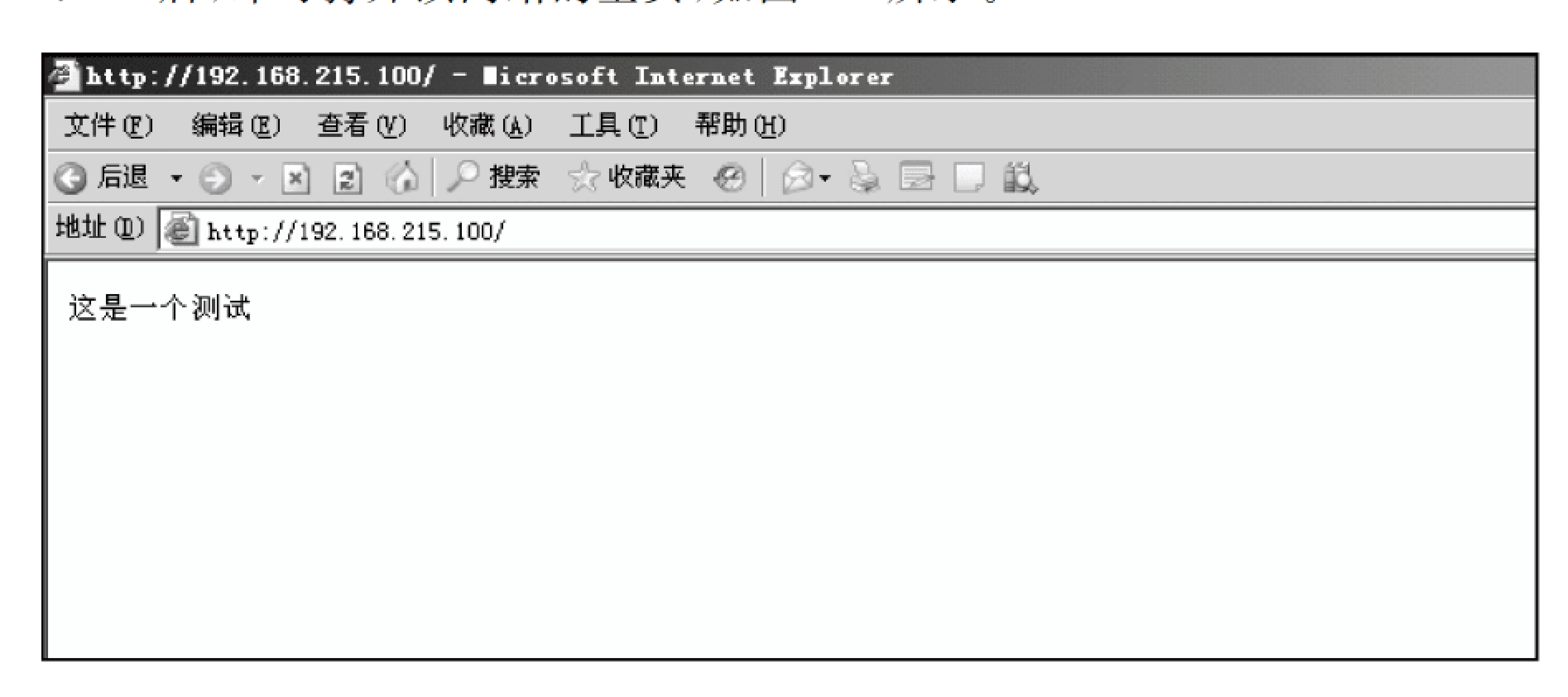


图 5-6 测试主页

4. 虚拟主机管理

所谓虚拟主机，就是把一台服务器划分成多个"虚拟"的服务器，每一个虚拟主机都具有独立的域名和完整的服务器(支持 WWW、FTP、E-mail 等)功能。一台服务器上的不同虚拟主机是各自独立的，并由用户自行管理。在外界看来，每一台虚拟主机和一台独立的主机完全一样。

要确保用户的请求能到达正确的网站，必须为服务器上的每个站点配置唯一的标识。要执行此操作，必须至少使用三个唯一标识符(主机头名称、IP 地址和唯一 TCP 端口号)中的一个来区分每个网站。通过更改这三个标识符中的一个，可以为多个网站创建唯一的标识，而无须为每个站点安装一个专用的服务器。也可以为每个站点创建唯一的主目录并且将内容存储在本地服务器或远程网络上，这样，每个网站都将作为一个虚拟服务器。在一台服务器上宿主多个网站可以节约硬件资源、节省空间和降低能源成本。Windows Server 2003 可以采用三种方式建立 Web 虚拟主机。

1) 使用多个 IP 地址创建多个站点

一些安全服务器配置要求在同一台服务器上使用唯一 IP 地址来区分每个站点。若想在同一台服务器上使用多个 IP 地址来区分不同的站点，则必须配置 IIS 来给每个站点指派唯一的 IP 地址。配置方法如下：

(1) 依次单击"开始"→"控制面板"→"网络连接"→"本地连接"，然后单击"属性"打开"本地连接属性"面板。

(2) 选择"Internet 协议(TCP/IP)"，单击"属性"打开"Internet 协议(TCP/IP)属性"对话框，单击下方的"高级"按钮打开"高级 TCP/IP 设置"对话框，可以发现 IP 地址栏中列出了已设定的 IP 地址和子网掩码。

(3) 单击"添加"按钮，在弹出的对话框中添加新的 IP 地址，子网掩码与原有的相同。然后依次单击"确定"按钮，就完成了多个 IP 地址的绑定。

(4) 用前面介绍的方法建立网站，各个网站分别选择不同的 IP 地址，网站 TCP 端口采用默认值"80"，网站的主机头采用默认值"无"。

2）使用主机头名创建多个站点

一般的 Web 服务器一个 IP 地址的 80 端口只能对应一个网站，处理一个域名的访问请求。在不使用多个 IP 地址和端口的情况下，如果要支持多个相对独立的网站就需要一种机制来分辨同一个 IP 地址上的不同网站的请求，这就是主机头绑定的方法。

主机头可以理解为每个网站的描述性名称，一台服务器上宿主多个网站的方法通常使用主机头，这是因为此方法可以节省 IP 地址资源。配置方法如下：

(1) 要使用主机头法必须先进行 DNS 设置，设置方法详见 5.1.2 节。

(2) 建立网站，其中 TCP 端口保持默认的 80 不变，"此站点的主机头"一项要填上该网站的域名，如图 5-7 所示。接着进行主目录选定、访问权限设置等操作，完成站点的设置，并用同样的方法建立其他网站。

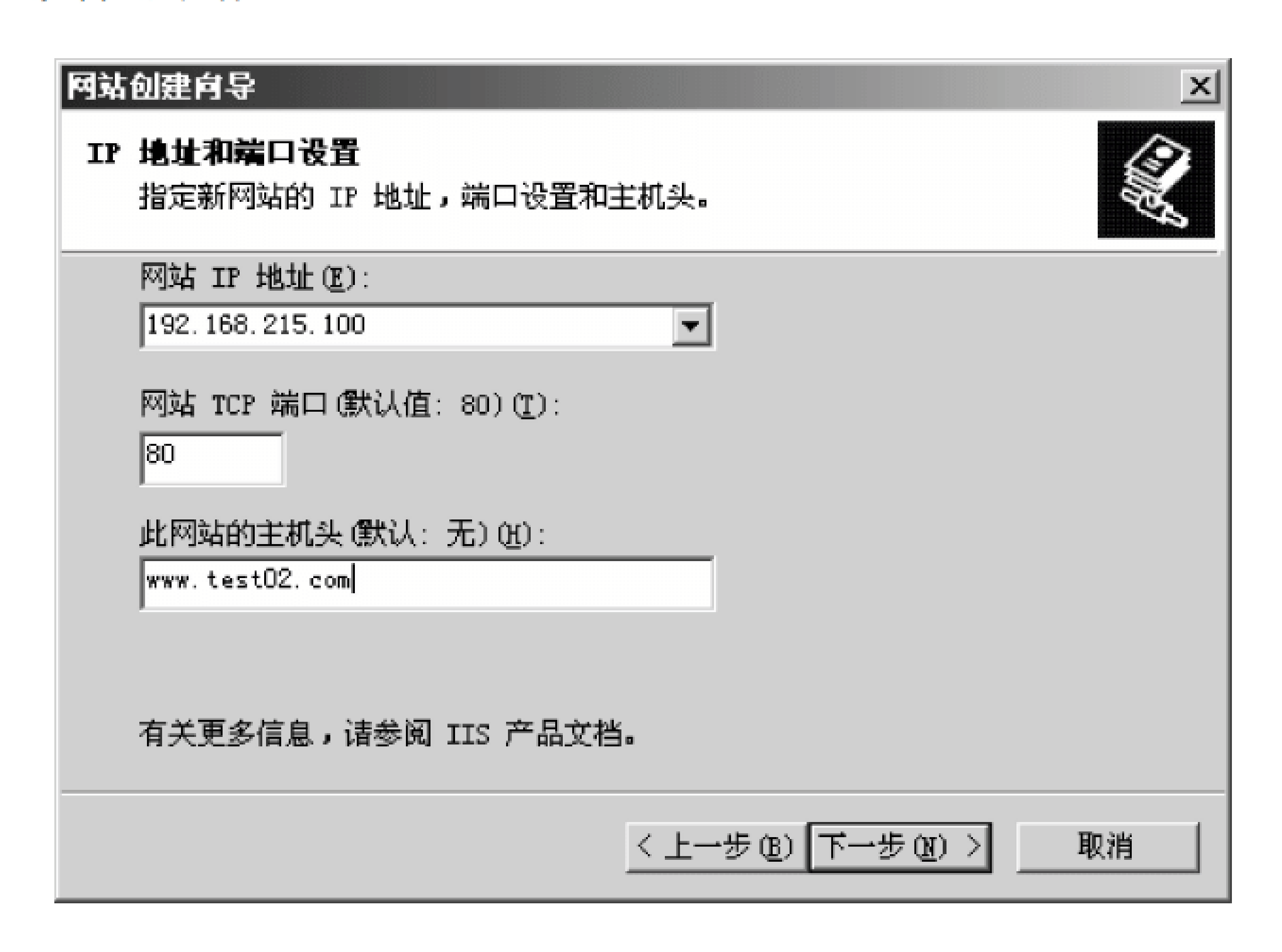


图 5-7　主机头设置

(3) 对已经建立好的网站，可以通过修改来配置主机头信息。在网站属性对话框中单击"高级"按钮，打开如图 5-8 所示的"高级网站标识"对话框。

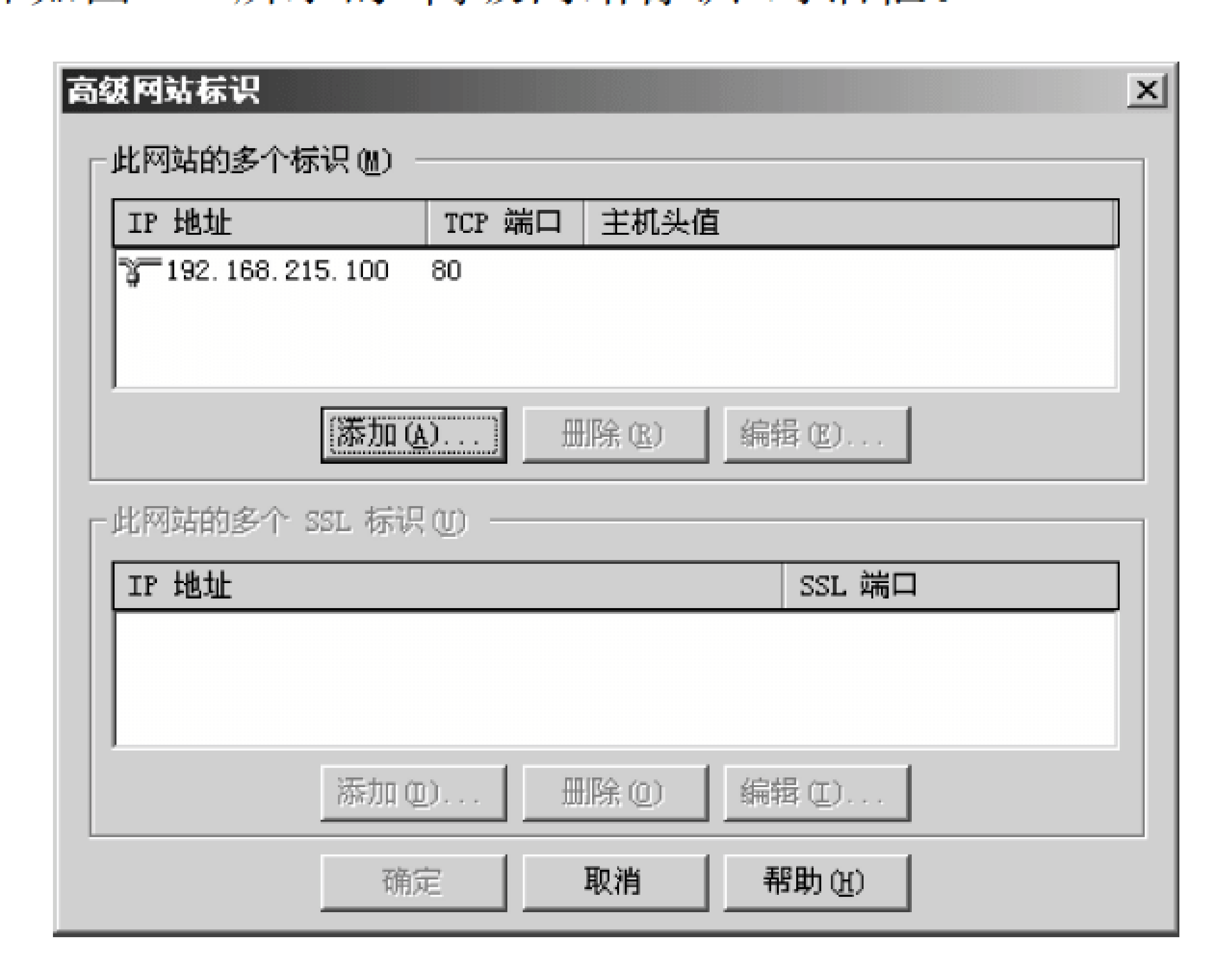


图 5-8　"高级网站标识"对话框

(4) 单击“添加”按钮,打开如图 5-9 所示的“添加/编辑网站标识”对话框,在其中添加相应的信息即可。

3) 使用端口号创建多个站点

通过同一个 IP 地址绑定不同端口号的方法也可以建立多个站点。标准网站默认的 TCP 端口号为 80,如果使用非标准 TCP 端口号来标识网站,用户访问站点时就必须知道指派给该网站的端口号,并需要把这个端口号附加在网站的名称或 IP 地址之后,如 http://192.168.215.100:8080。操作方法可以在上面的基础上进行修改,如图 5-10 所示。



图 5-9 “添加/编辑网站标识”对话框

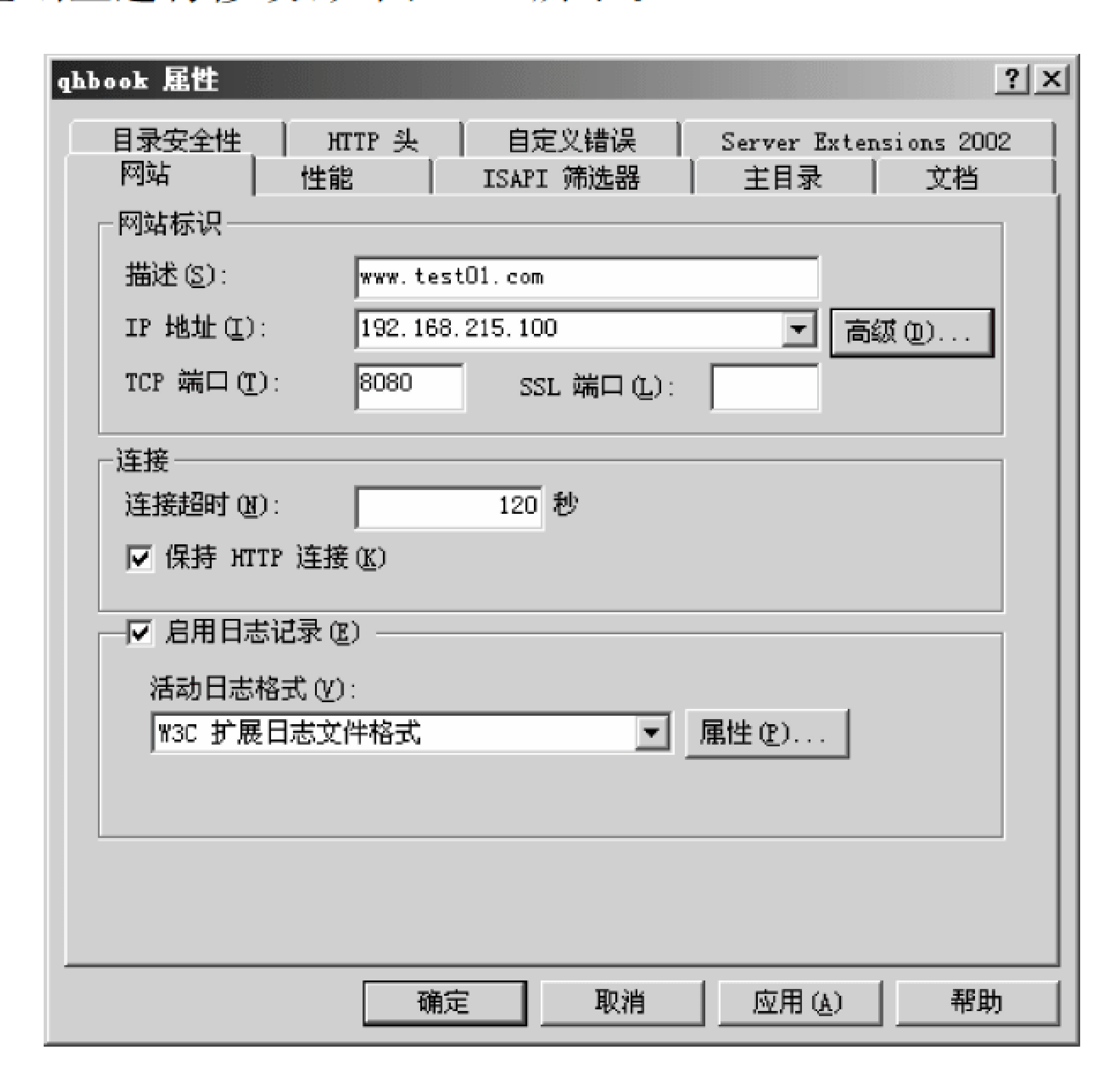


图 5-10 端口配置对话框

5. 虚拟目录管理

1) 虚拟目录概述

Internet 服务可以从多个目录发布,通过通用命名约定名(UNC)、用户名及用于访问权限的密码指定目录,可将每个目录定位在本地驱动器或网络上。通常,服务器可拥有一个宿主目录和任意数量的其他发布目录,其他发布目录称为虚拟目录。

虚拟目录是相对于 IIS 的根目录来说的,一个站点的根目录只能有一个,为了能使多个 Web 服务运行于同一个 IIS 服务器上,就需要为其虚拟一个 IIS 目录。每个虚拟目录受控于根目录的管理,有其特定的管理权限,也可以继承根目录的权限设置。每个虚拟目录的程序有其相对隔离的进程运行空间,保证了程序的安全运行。当然,每个虚拟目录都是指向物理磁盘中的绝对路径的,而虚拟目录指向的绝对路径可以是任意的。

2) 虚拟目录配置

(1) 打开“Internet 信息服务(IIS)管理器”窗口;选中“站点”,右击后用鼠标左键单击

“新建”→“虚拟目录”命令，如图 5-11 所示；打开“虚拟目录创建向导”对话框，单击“下一步”按钮。

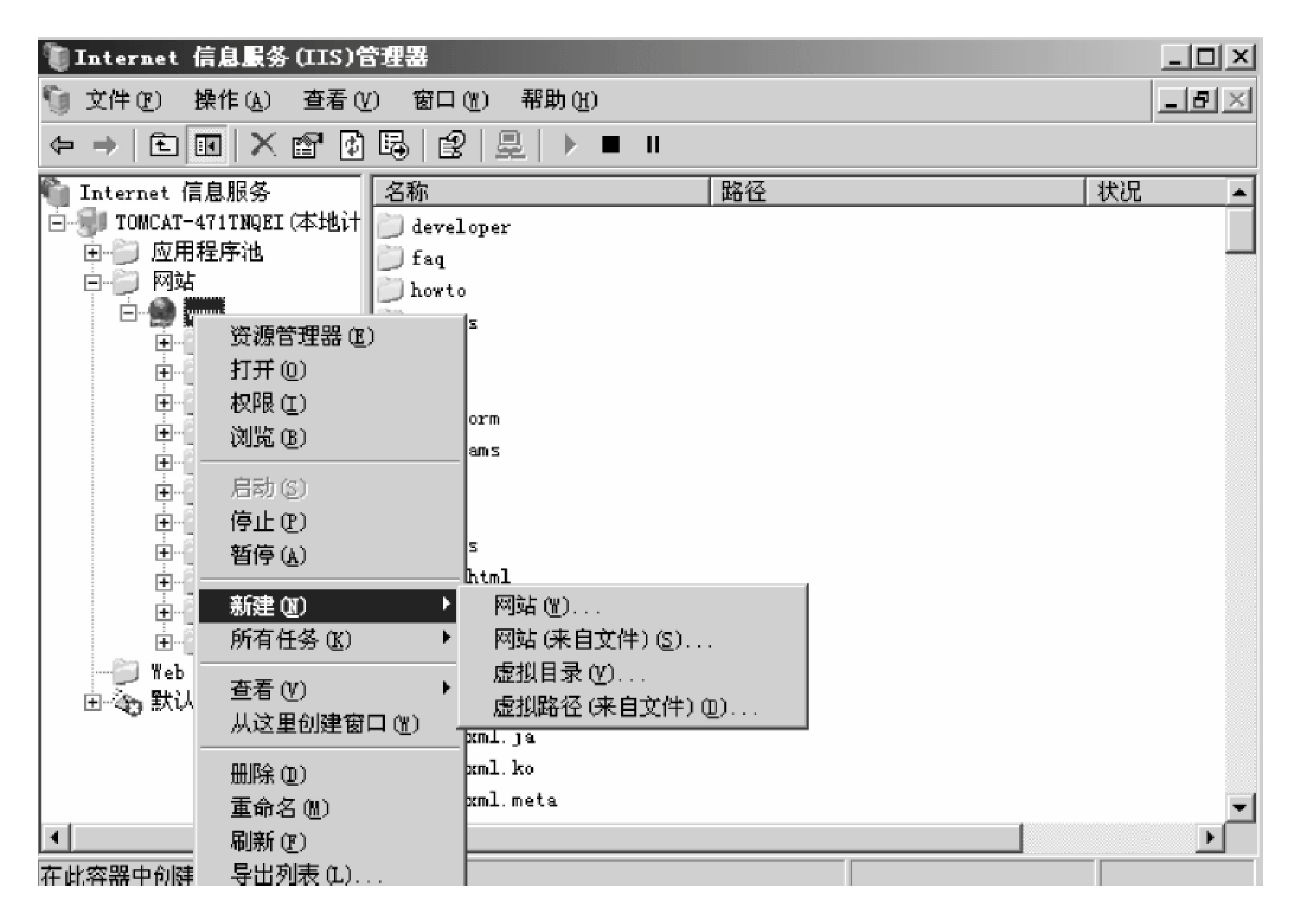


图 5-11 “Internet 信息服务(IIS)管理器”窗口

(2) 在如图 5-12 所示的“虚拟目录别名”对话框中，输入所要创建的虚拟目录的别名，单击“下一步”按钮。

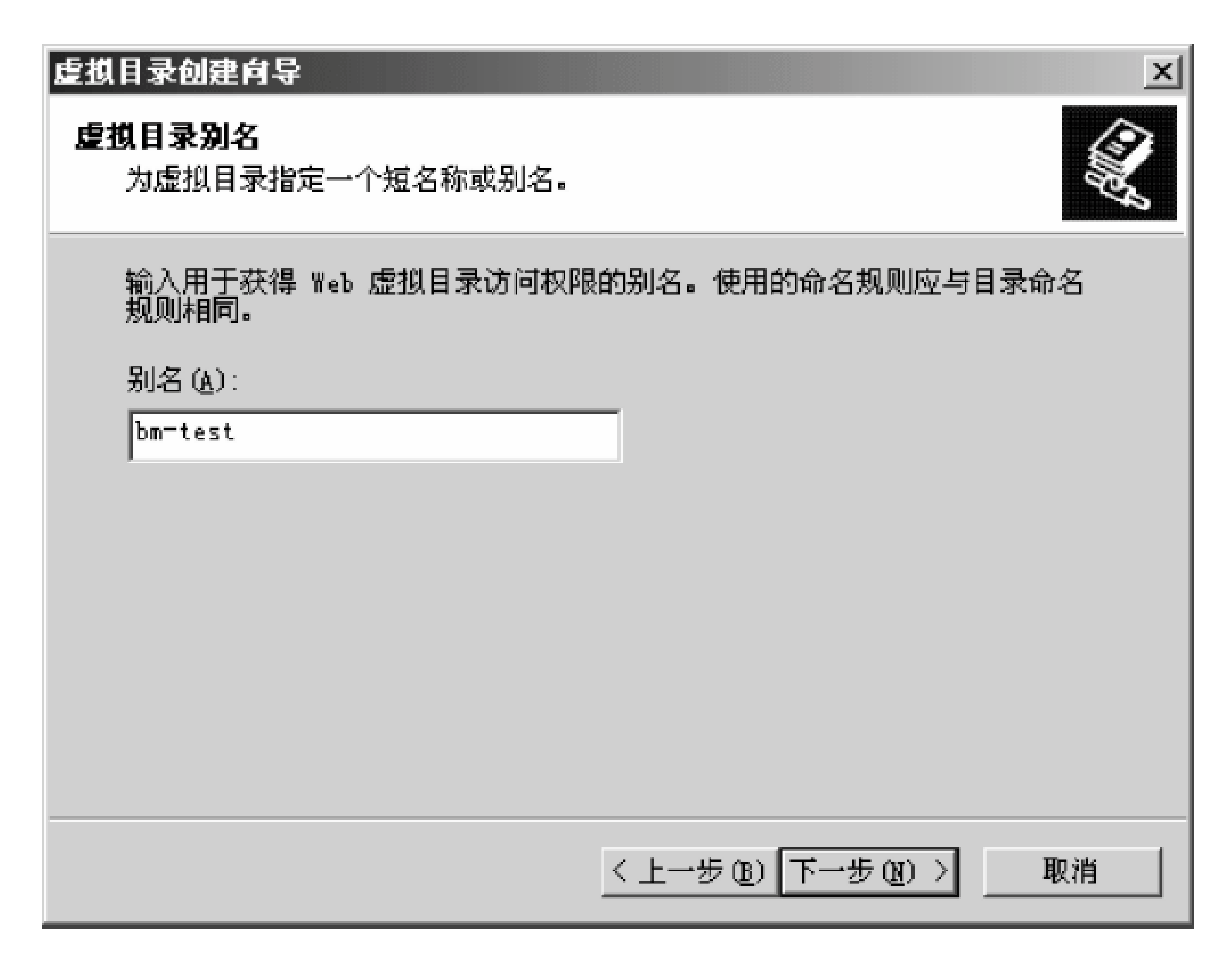


图 5-12 “虚拟目录别名”对话框

(3) 在“网站内容目录”对话框的“路径”文本框中输入目录的物理路径，或通过“浏览”按钮定位目录的物理路径。

(4) 在“虚拟目录访问权限”对话框中，设置虚拟目录的适当权限，从安全性考虑通常建议只允许“读取”和“浏览”。

(5) 单击“完成”按扭完成虚拟目录的设置。这时可以看到在“默认站点”里多了一个虚拟目录及该目录中的文件。虚拟目录可以隐含物理目录,从而提高目录的安全性。对虚拟目录的访问如同访问实际目录一样,只要在浏览器的地址栏中输入 IP 地址或域名即可打开 Web 站点下的虚拟目录。

5.1.2 DNS 服务器管理

1. 安装 DNS 服务器

默认情况下 Windows Server 2003 系统中并没有安装 DNS 组件,必须自己安装,方法如下:

(1) 依次单击“开始”→“管理工具”→“配置您的服务器向导”,在打开的对话框中单击“下一步”按钮。配置向导自动检测所有网络连接的设置情况,若没有发现问题则进入“服务器角色” 对话框。

(2) 在“服务器角色”列表中单击“DNS 服务器”选项,并单击“下一步”按钮。打开“选择总结” 对话框,如果列表中出现“安装 DNS 服务器”和“运行配置 DNS 服务器向导来配置 DNS”,则直接单击“下一步”按钮。

(3) 向导开始安装 DNS 服务器,并且可能会提示插入 Windows Server 2003 的安装光盘或指定安装源文件。

2. 创建区域

DNS 服务器安装完成以后会自动打开“配置 DNS 服务器向导”对话框,用户可以在该向导的指引下创建区域。

(1) 在“配置 DNS 服务器向导”的欢迎对话框中单击“下一步”按钮,打开“选择配置操作”对话框。选中适合小型网络使用的“创建正向查找区域”单选按钮,并单击“下一步”按钮。

(2) 打开“主服务器位置”对话框,如果所部署的 DNS 服务器是网络中的第一台 DNS 服务器,则应该保持“这台服务器维护该区域”单选按钮的选中状态,将该 DNS 服务器作为主 DNS 服务器使用,并单击“下一步”按钮。

(3) 打开“区域名称”对话框,在“区域名称”文本框中输入一个能反映企业信息的区域名称,如图 5-13 所示,然后单击“下一步”按钮。

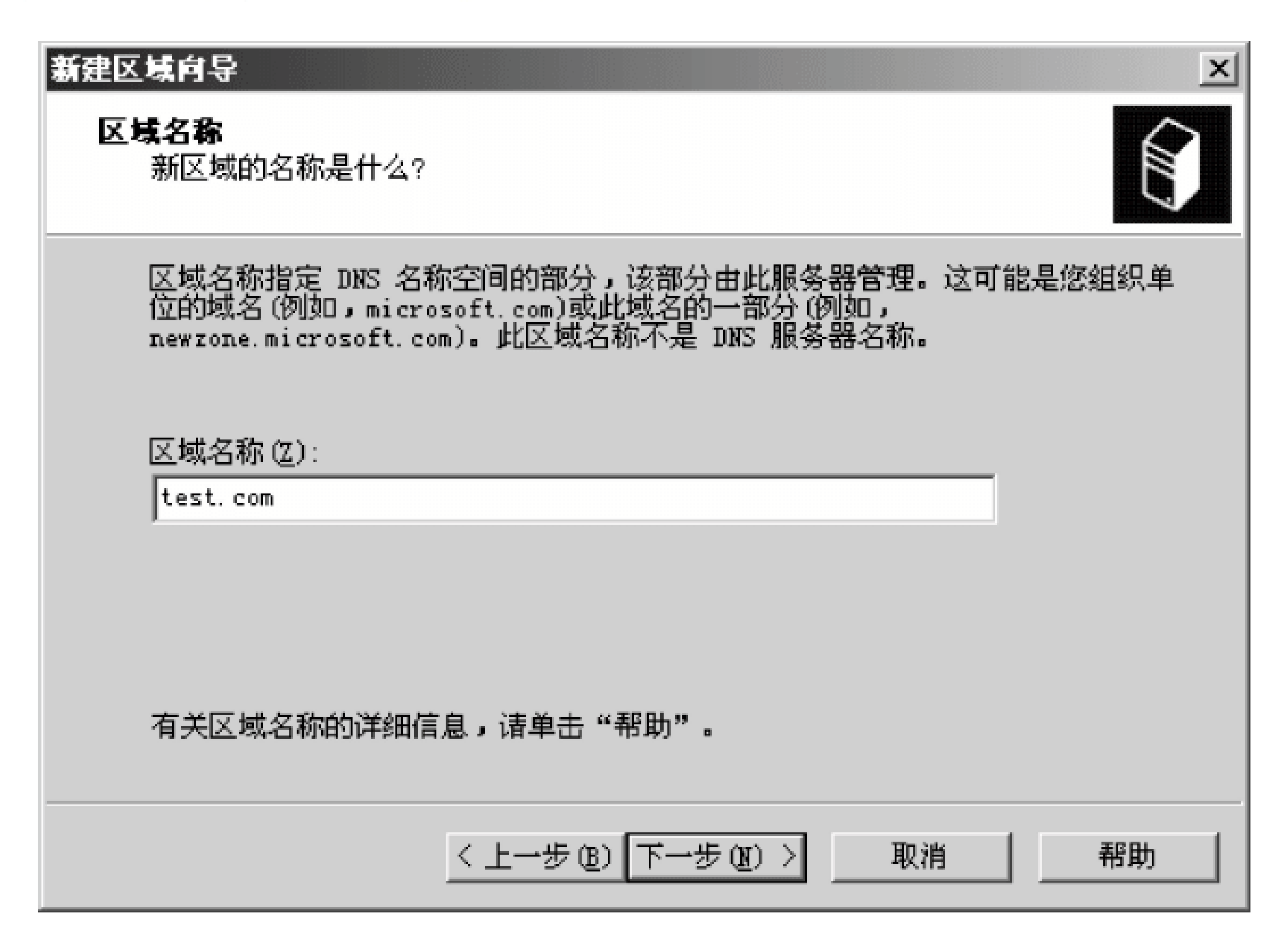


图 5-13 填写区域名称

(4) 在打开的"区域文件"对话框中已经根据区域名称默认填入了一个文件名。该文件是一个 ASCII 文本文件,里面保存着该区域的信息,默认情况下保存在 windowssystem32dns 文件夹中。保持默认值不变,单击"下一步"按钮。

(5) 在打开的"动态更新" 对话框中指定该 DNS 区域能够接受的注册信息更新类型。允许动态更新可以让系统自动地在 DNS 中注册有关信息,在实际应用中比较有用,因此选中"允许非安全和安全动态更新"单选按钮,单击"下一步"按钮。

(6) 打开"转发器"对话框,如图 5-14 所示。通过配置"转发器"可以使内部用户在访问 Internet 上的站点时使用当地的 ISP 提供的 DNS 服务器进行域名解析。这里保持"是,应当将查询转发到有下列 IP 地址的 DNS 服务器上"单选按钮的选中状态。在 IP 地址文本框中输入 ISP(或上级 DNS 服务器)提供的 DNS 服务器的 IP 地址,单击"下一步"按钮。

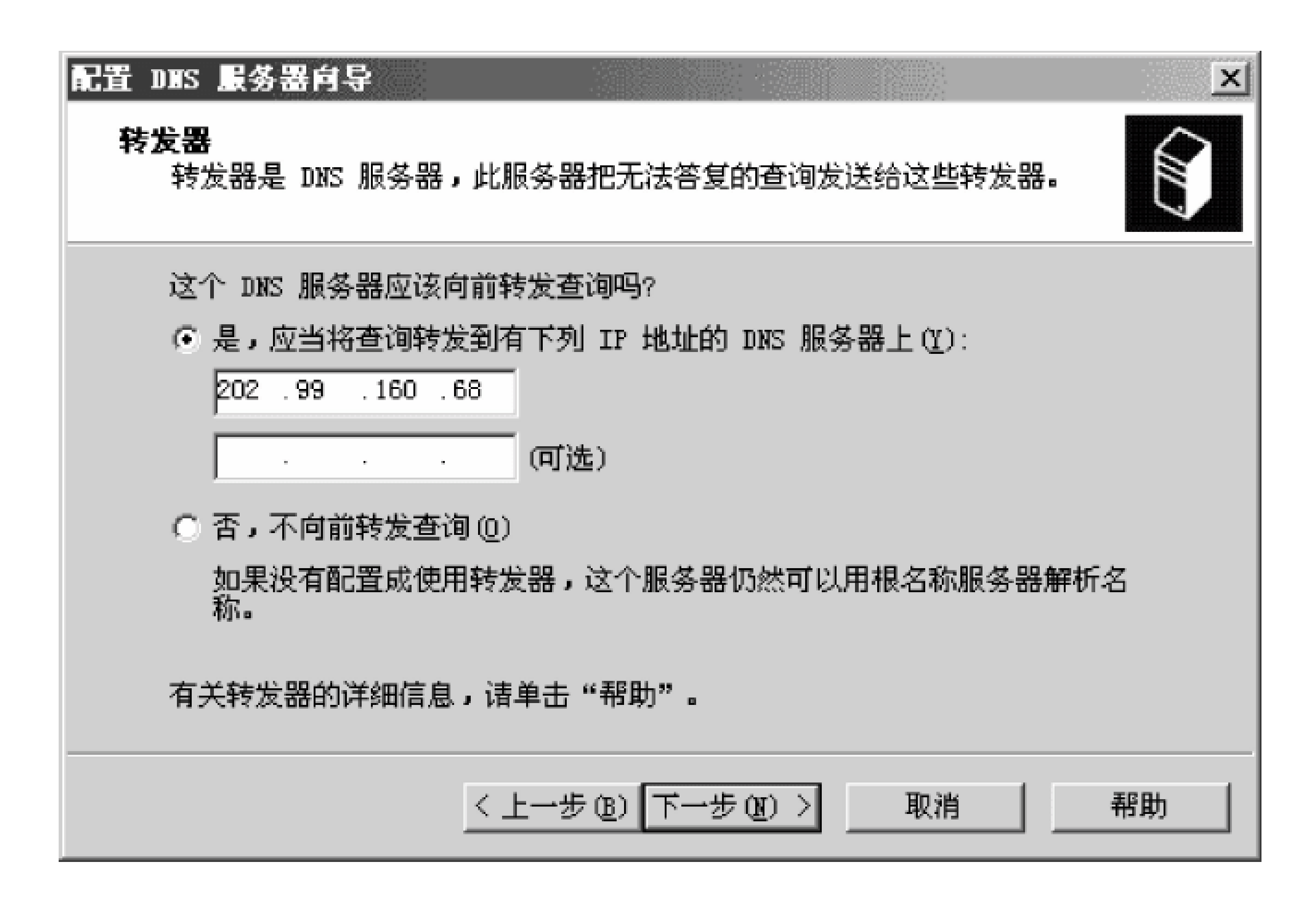


图 5-14　配置 DNS 转发

(7) 依次单击"完成"按钮结束区域的创建过程和 DNS 服务器的安装配置过程。

3. 创建域名

虽然利用向导成功地创建了 test. com 区域,但是此时内部用户还不能使用这个名称来访问内部站点,因为它还不是一个合格的域名。所以需要在其基础上创建指向不同主机的域名才能提供域名解析服务。创建域名 www. test. com 操作的步骤如下:

(1) 依次单击"开始"→"管理工具"→DNS 菜单命令,打开 dnsmagt 控制台窗口。

(2) 在左窗格中依次展开 ServerName→"正向查找区域"目录。然后单击 test. com 区域,执行快捷菜单中的"新建主机"命令。

(3) 打开"新建主机"对话框,如图 5-15 所示。在"名称"(如果为空则使用其父域名称)文本框中输入一个能代表该主机所提供服务的名称(如 www)。在"IP 地址"文本框中输入该主机的 IP 地址,单击"添加主机"按钮。很快就会提示已经成功创建了主机记录。

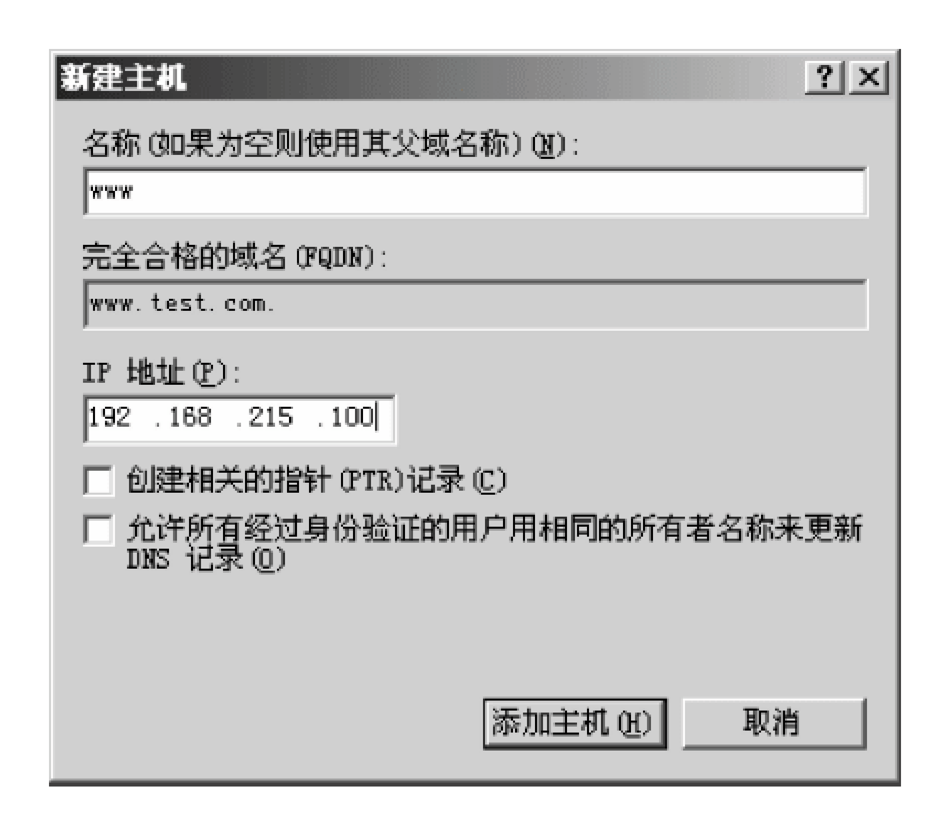


图 5-15　"新建主机"对话框

(4) 最后单击“完成”按钮结束 DNS 域名的创建。

4. 设置 DNS 客户端

尽管 DNS 服务器已经创建成功，并且也已经创建了合适的域名，但是在客户机的浏览器中仍无法使用 www.test.com 这样的域名访问网站。这是因为虽然已经有了 DNS 服务器，但客户机并不知道 DNS 服务器在哪里，因此不能识别用户输入的域名。必须手动设置 DNS 服务器的 IP 地址才行。在客户机“Internet 协议(TCP/IP)属性”对话框中的“首选 DNS 服务器”文本框中设置刚刚部署的 DNS 服务器的 IP 地址，如图 5-16 所示。然后单击“确定”按钮完成客户端的配置。

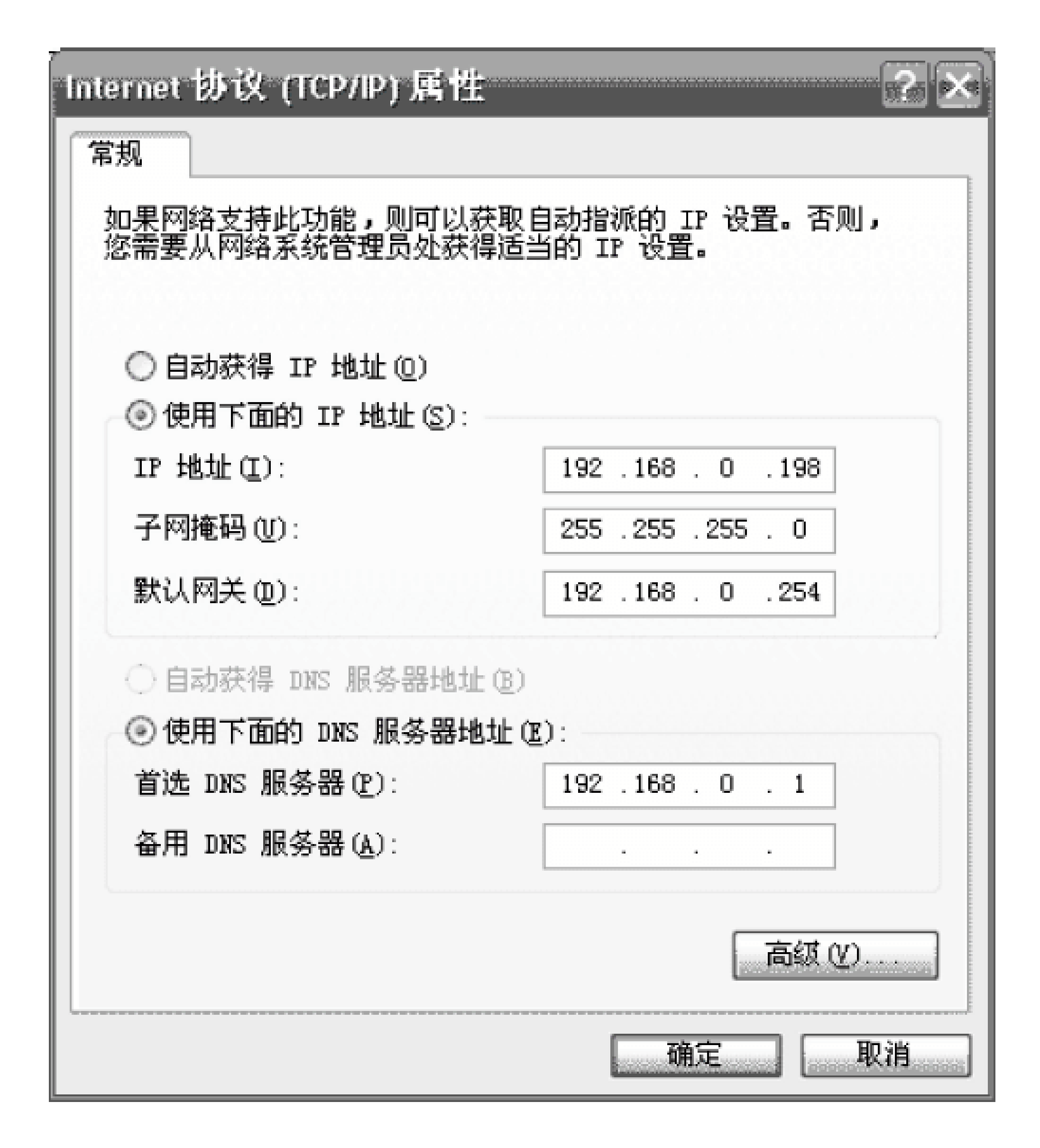


图 5-16 设置客户端 DNS 服务器地址

5.1.3 邮件服务器管理

邮件服务器也是企业网络管理中的任务之一。与 Web 网站、FTP 站点服务器一样，邮件服务器的配置方案也非常多，下面介绍的是基于 Windows Server 2003 的邮件服务器管理。

1. 邮件服务器的安装

邮件服务器系统由 POP3 服务、SMTP 服务以及电子邮件客户端三个组件组成。其中的 POP3 服务与 SMTP 服务一起使用，POP3 为用户提供邮件下载服务，而 SMTP 则用于发送邮件以及邮件在服务器之间的传递。电子邮件客户端是用于读取、撰写以及管理电子邮件的软件。Windows Server 2003 的 POP3 服务组件可以使用户无须借助任何工具软件，即可搭建一个邮件服务器，方法如下：

(1) 选择“开始”→“管理工具”，打开“配置您的服务器向导”对话框。

(2) 单击“下一步”按钮，打开“预备步骤”提示对话框，在其中提示了在进行以下步骤前需要做好的准备工作。

(3) 单击“下一步”按钮，打开“服务器角色”对话框。在其中选择“邮件服务器(POP3, SMTP)”选项，如图 5-17 所示。

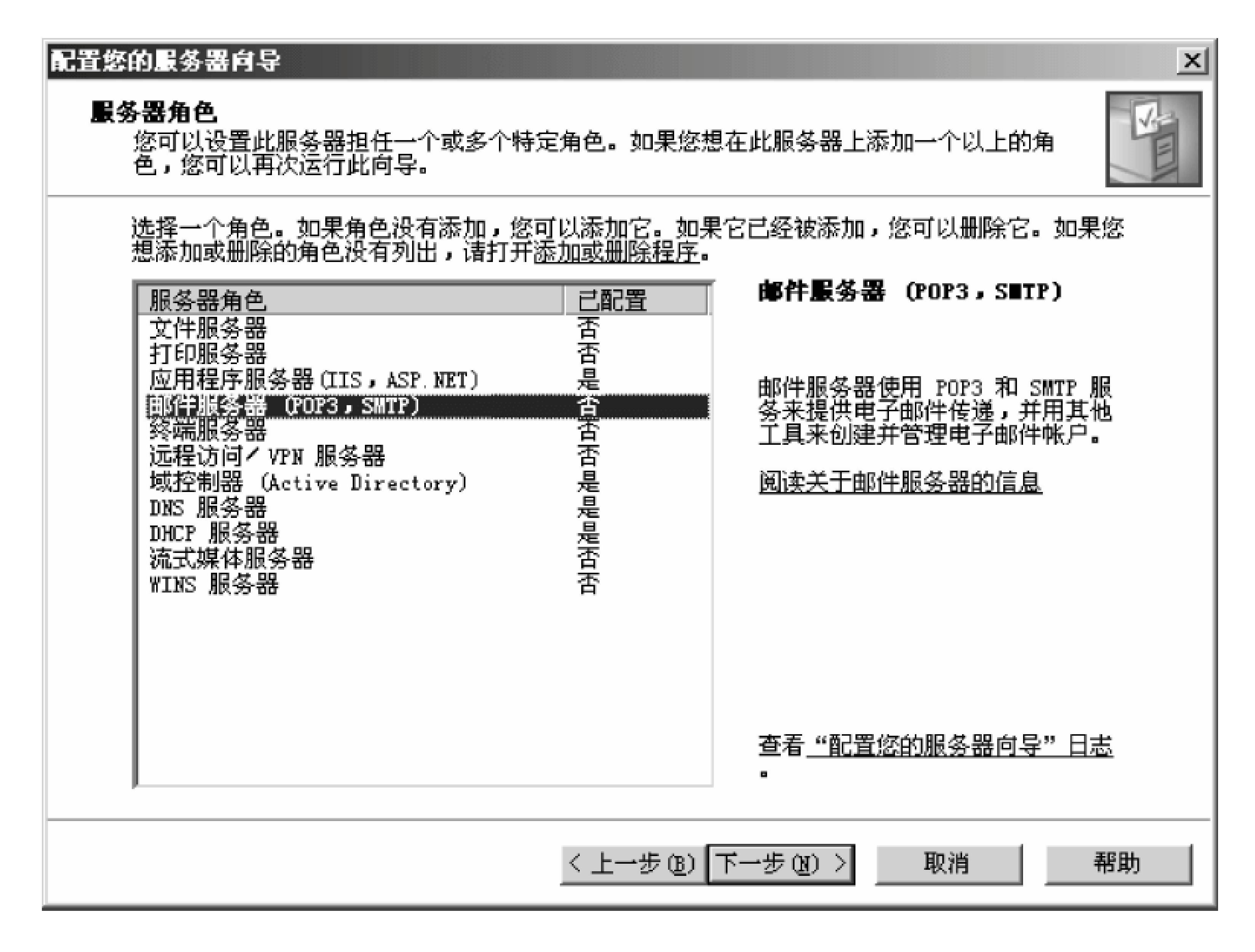


图 5-17 “服务器角色”对话框

(4) 单击“下一步”按钮，打开如图 5-18 所示的对话框。在其中要求选择邮件服务器中所使用的用户身份验证方法，如果是在域网络中，选择“Active Directory 集成的”方式，然后在“电子邮件域名”中指定一个邮件服务器名。

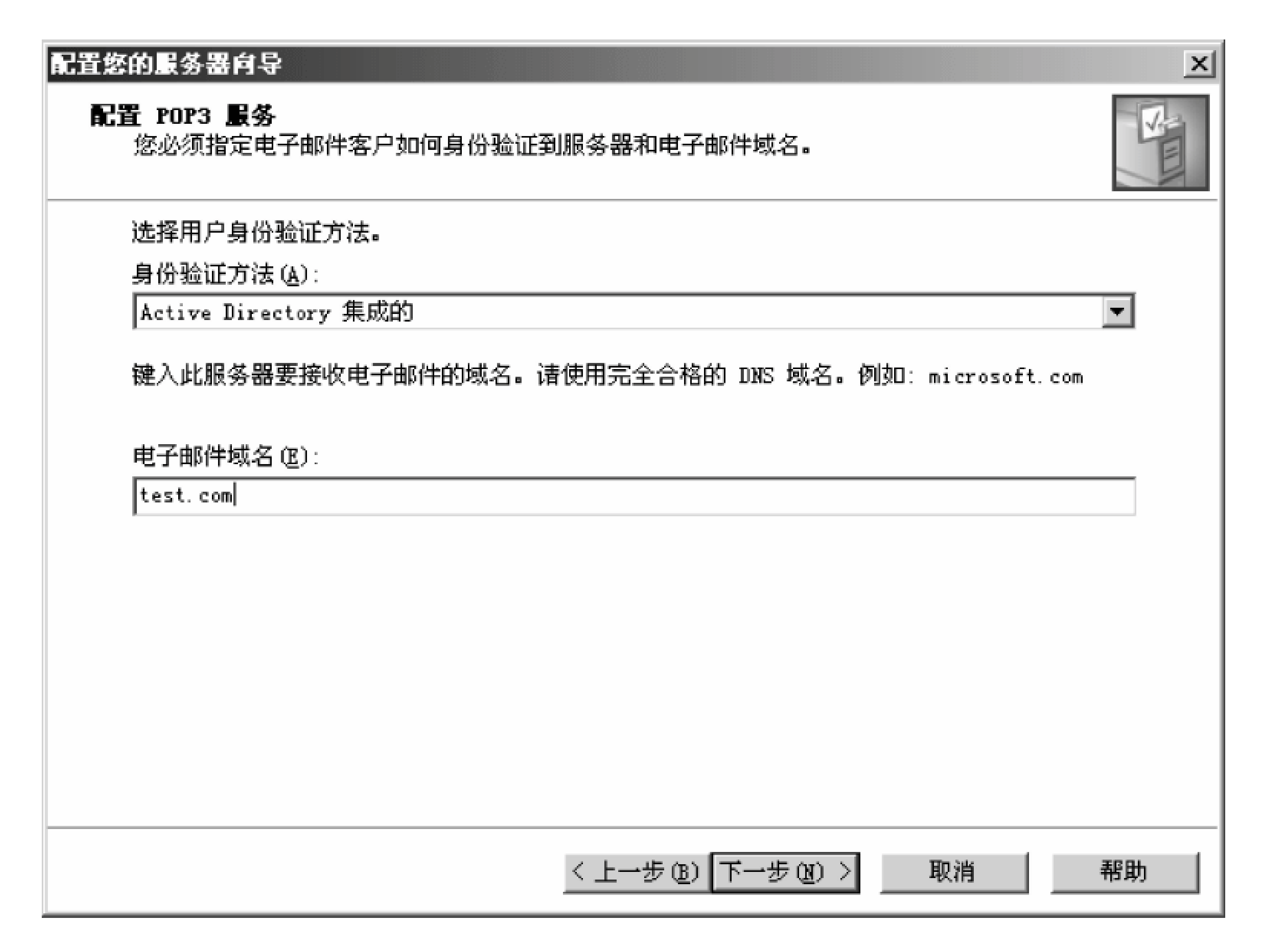


图 5-18 “配置 POP3 服务”对话框

(5) 单击“下一步”按钮，打开“选择总结”对话框，在列表中总结了以上配置选择。

(6) 单击“下一步”按钮后系统开始安装邮件服务器所需的组件。在此过程中，系统会提示用户指定 Windows Server 2003 系统源程序所在位置，以便复制所需文件。

(7) 完成文件复制后,直接单击"完成"按钮完成邮件服务器的整个安装过程。完成后执行"开始"→"管理工具"→"管理您的服务器"菜单操作,在打开的"管理您的服务器"窗口即可见到刚才安装的邮件服务器。单击"管理此邮件服务器"即可打开"POP3 服务"窗口,如图 5-19 所示。

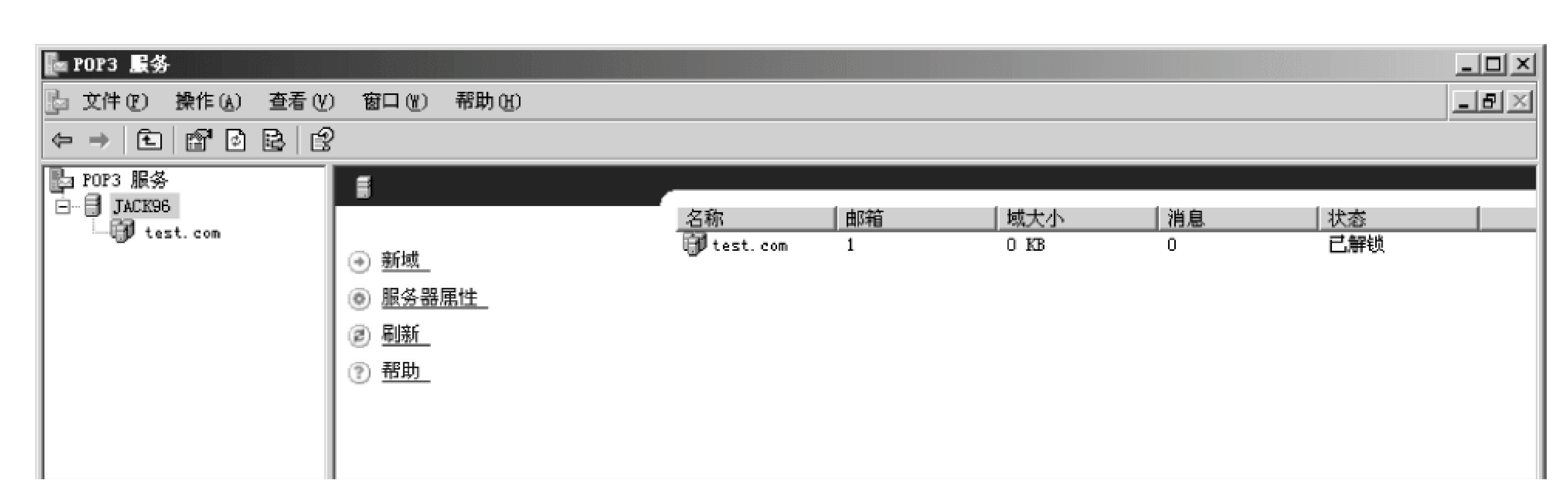


图 5-19 "POP3 服务"窗口

2. 邮件服务器的配置

邮件服务器安装好后还需要进行一定的配置才能正常工作。配置步骤为:

(1) 执行"开始"→"管理工具"→"POP3 服务"菜单操作,打开邮件服务器窗口。

(2) 在"POP3 服务"窗口左边单击邮件服务器名,然后单击右键,在弹出的快捷菜单中选择"属性",或者在右边窗格中单击"服务器属性"链接,打开如图 5-20 所示的邮件服务器属性对话框。

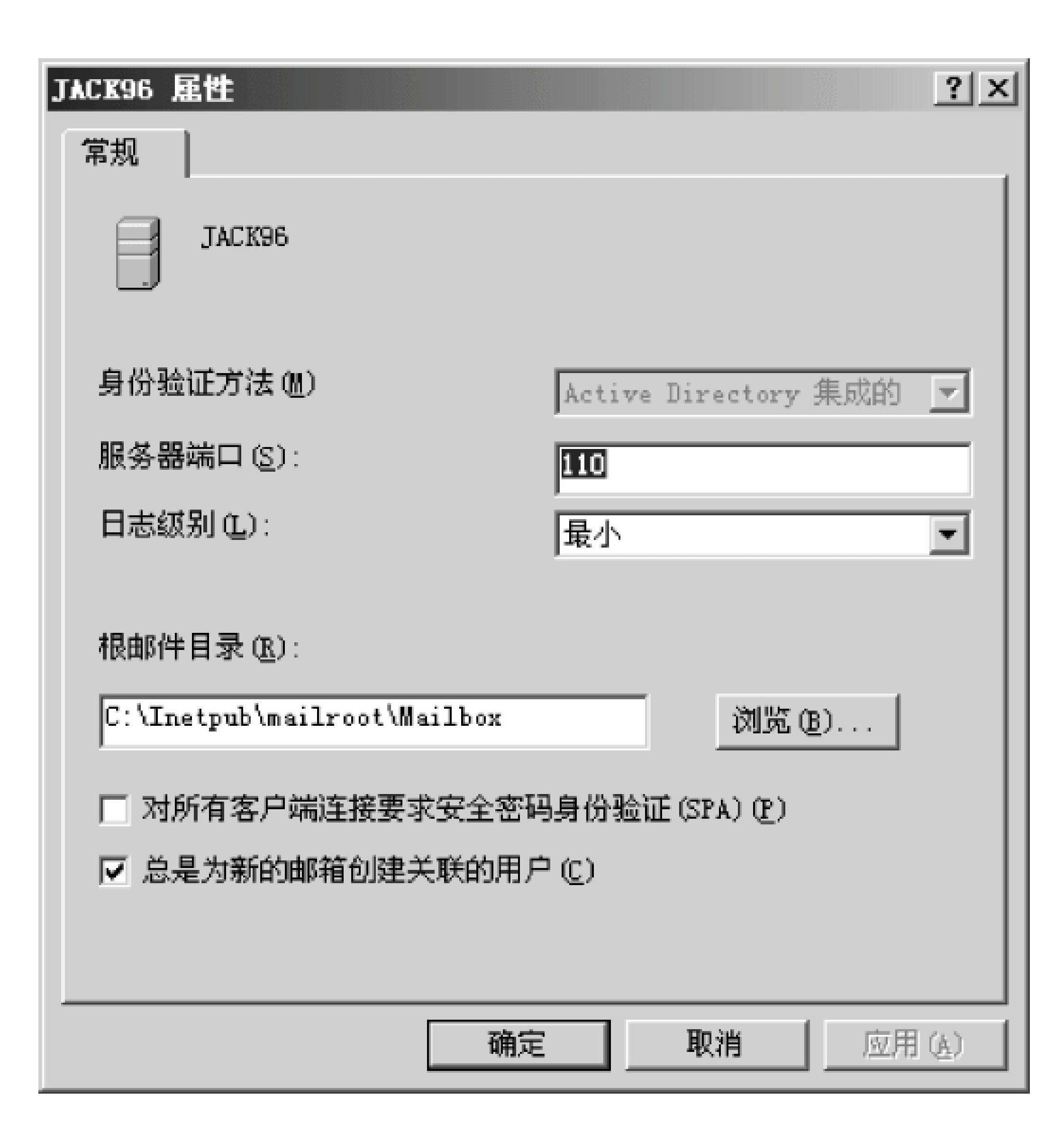


图 5-20 邮件服务器属性对话框

在该对话框中可以配置服务器所使用的端口、日志级别、根邮件目录,是否要采取安全密码身份验证方式,以及是否为新邮箱创建关联的用户。

(3) 在邮件服务器窗口左边窗格中选择相应的邮件服务器域名,在右边窗格中单击"添加邮箱"链接。在这里可以添加新用户邮箱,如果要同时为系统创建一个用户账户,则要选

择“为此邮箱创建相关联的用户”复选框，输入好邮箱名和密码后单击“确定”按钮，完成邮件服务器的配置。

3. 邮件服务器的管理

在邮件服务器安装过程中，将添加并设置一个新的域名，以将它用于 E-mail 服务。如果企业申请有两个或多个域名，或者该服务器作为虚拟主机来提供邮件服务，也可以添加多个域名以实现多邮件虚拟服务的共存。

1）创建域

（1）打开“POP3 服务”窗口，鼠标右键单击其中的“计算机名”节点，并在弹出的快捷菜单中选择“新建”→“域”选项，在“添加域”对话框中的“域名”文本框中输入新域名，并确保该域名已经在 DNS 服务中设置好 MX 记录。

（2）单击该对话框中的“确定”按钮，以完成新域名的添加。

（3）重复上述操作，可在邮件服务器中添加多个域名。

2）管理域

在一个 POP3 窗口中，可以对电子邮件域进行必要的管理，例如删除、锁定/解除锁定。操作方法为：

（1）在“POP3 服务”窗口中，单击“计算机名”，并且右键单击要删除的域，然后单击“删除”菜单命令，根据提示即可删除该域、域中所有邮箱以及存储在域中的所有邮件。

（2）鼠标右键单击要锁定的域，从快捷菜单中选择“锁定”菜单命令，即锁定了该域。

（3）在解除锁定域时，只需再从快捷菜单中选择“解除锁定”菜单命令即可。

3）管理邮箱

在建立了一个邮件域之后，就可以在该域中建立账户（即邮箱账户），并对邮箱进行管理。

（1）创建邮箱

打开“POP3 服务”窗口，选中要创建新邮箱的域，然后在右键快捷菜单中依次选择“新建”→“邮箱”子菜单。或者在如图 5-21 所示的窗口中，单击“添加邮箱”链接，在弹出的对话框中输入“邮箱名”，同时在“密码”及“确认密码”框中输入相同的密码；最后单击“确定”按钮，即完成邮箱的添加工作。重复上述操作，可以为所有网络用户都添加电子邮箱。

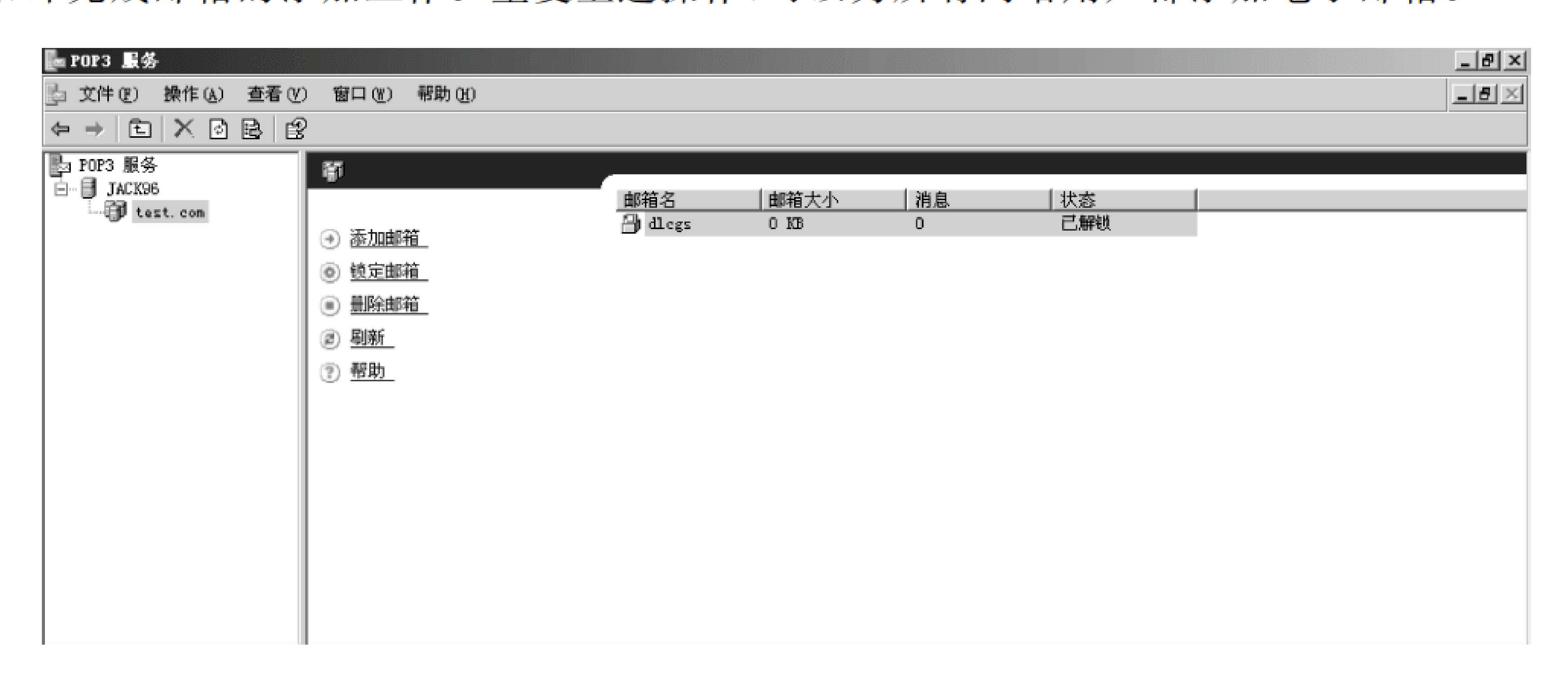


图 5-21　邮件服务器属性窗口

(2) 删除邮箱

在图 5-21 中单击“删除邮箱”链接,将弹出“删除邮箱”对话框,以询问是否“同时也删除与此邮箱相关联的用户账户”。如果选中该复选框,则 Users 组中的该用户也同时被删除。这也就是说,将同时剥夺该用户访问发送电子邮件服务器和登录至域的权限。

最后单击“是”按钮,删除该邮箱成功,同时也将删除该邮箱的邮件存储目录以及该目录中存储的所有电子邮件。

(3) 锁定/解除锁定邮箱

如果需要暂时禁用某个邮箱账户,但又没必要删除,以备日后重新启用,这时可以暂时锁定该邮箱账户。当一个邮箱被锁定时,仍然能接收发送到邮件存储区的传入电子邮件。但是,该用户却不能连接到服务器检索电子邮件。锁定一个邮箱只是限制了该用户使其不能连接到服务器,但是管理员仍然可以执行所有的管理任务。锁定/解除锁定邮箱的方法为:

在“POP3 服务”窗口中右击要锁定的信箱,并在弹出的快捷菜单中选择“锁定”子菜单。或单击“锁定邮箱”链接即可锁定该信箱。若要解除对该邮箱的锁定,只需在弹出的快捷菜单中选择“解除锁定”子菜单即可。

(4) 邮箱属性设置

用户对信箱最关心的事情莫过于其容量的大小以及安全问题。Windows Server 2003 的 POP3 邮件服务器可以通过启用磁盘配额,来限制一个账户的磁盘空间,以实现对邮箱大小的设置。同时还可以更改邮箱初始密码,这有效地保障了服务器及用户的利益。既防止了用户无限制地使用磁盘空间,又保护了用户邮件的安全。

(5) 邮箱大小设置

如果邮件服务器采用活动目录集成的身份验证或本地 Windows 账户身份验证,那么在为用户创建邮箱时,默认将创建一个配额文件,并启用相应的磁盘配额。因此,如果用户信箱采用默认的磁盘限额设置,就不必再为每个用户进行单独的设置。

- 启用磁盘配额功能:由于磁盘配额功能默认适用于全部电子邮箱,因此应当充分考虑到磁盘的总容量、用户总数量等因素,以合理地设置磁盘配额功能。
- 为个别用户单独设置磁盘配额:对于一些对邮箱容量有特殊要求的用户,可以单独为其设置磁盘配额。

5.1.4 FTP 管理

1. FTP 服务器的建立

(1) 依次单击“开始”→“设置”→“控制面板”→“添加/删除程序”,打开“添加/删除程序”对话框,选中“添加/删除 Windows 组件”。

(2) 在对话框中选中“Internet 信息服务(IIS)”,查看其详细信息,然后选中“文件传输协议(FTP)服务器”项后,单击“确定”按钮,接下来按照向导至安装完成,如图 5-22 所示。

(3) 依次单击“开始”→“程序”→“管理工具”→“Internet 信息服务”,打开 IIS 控制台。

(4) 右击“默认 FTP 站点”,在快捷菜单中选中“属性”命令,打开“默认 FTP 站点属性”对话框。在“FTP 站点”选项卡中,修改“描述”为容易识别的标识,“IP 地址”修改为当前主



图 5-22 “Internet 信息服务(IIS)管理器”窗口

机的某个 IP 地址(在主机具备多 IP 地址的情况下)。如图 5-23 所示,本机私有地址为“192.168.215.100”,“TCP 端口”为默认的 FTP 端口号“21”。

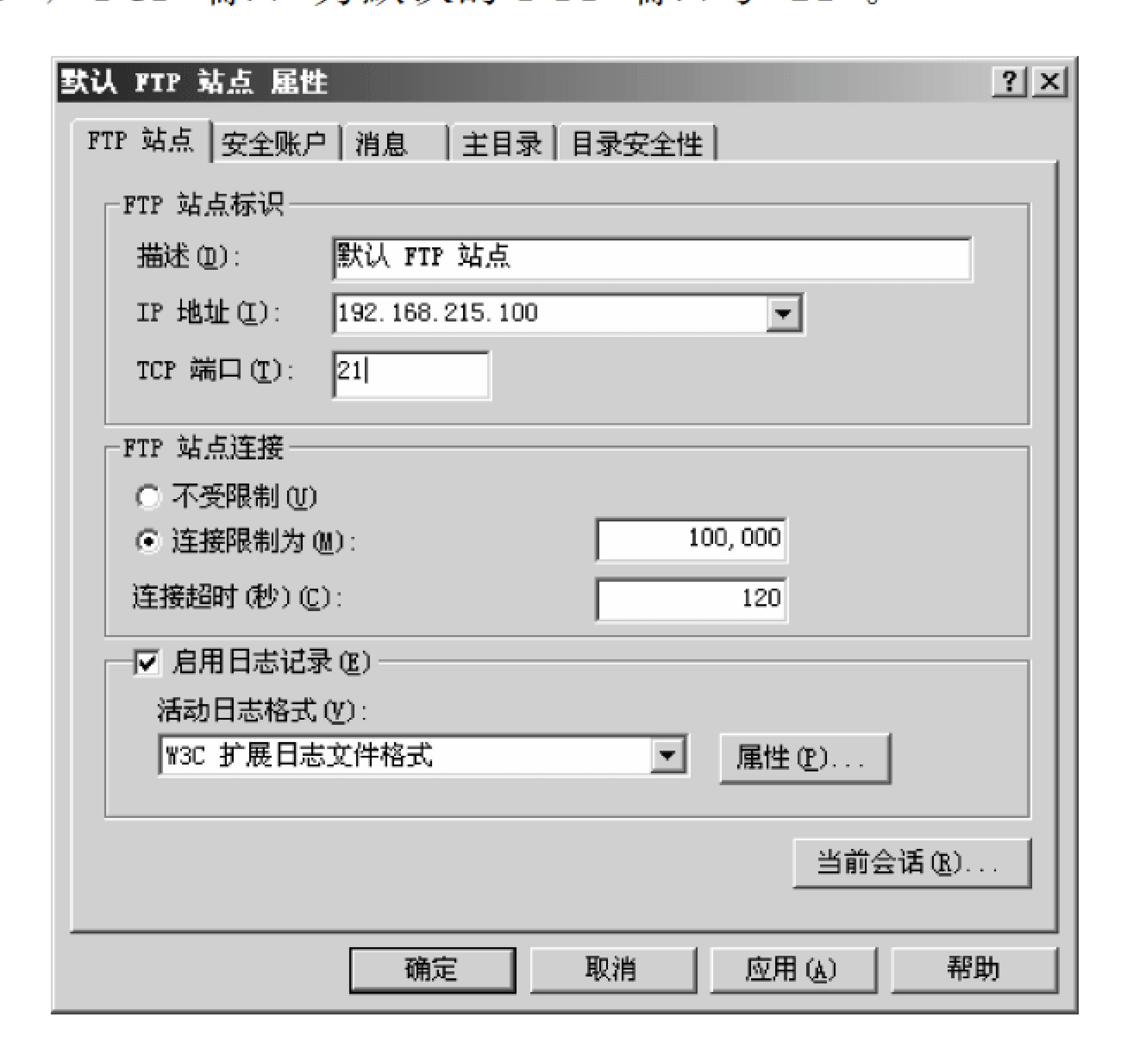


图 5-23 “FTP 站点”选项卡

(5) 在“安全账户”选项卡中选中“允许匿名连接”,如果客户端登录时需要进行身份验证,则可通过“浏览”来选中服务器的 Windows 用户。

(6) 在“消息”选项卡中添加 FTP 服务器的登录欢迎信息和退出信息。

(7) 在“主目录”选项卡中选择 FTP 服务器向外提供服务的主目录,此处可选择“此计

算机上的目录”。如果选择“另一台计算机上的目录”,则主目录在其他主机上,格式为“\\{服务器}\{共享名}”。FTP 站点目录下的“读取”、“写入”、“记录访问”选项可对访问权限进行控制,出于安全考虑应该为匿名 anonymous 用户分配“读取”权限,如图 5-24 所示。

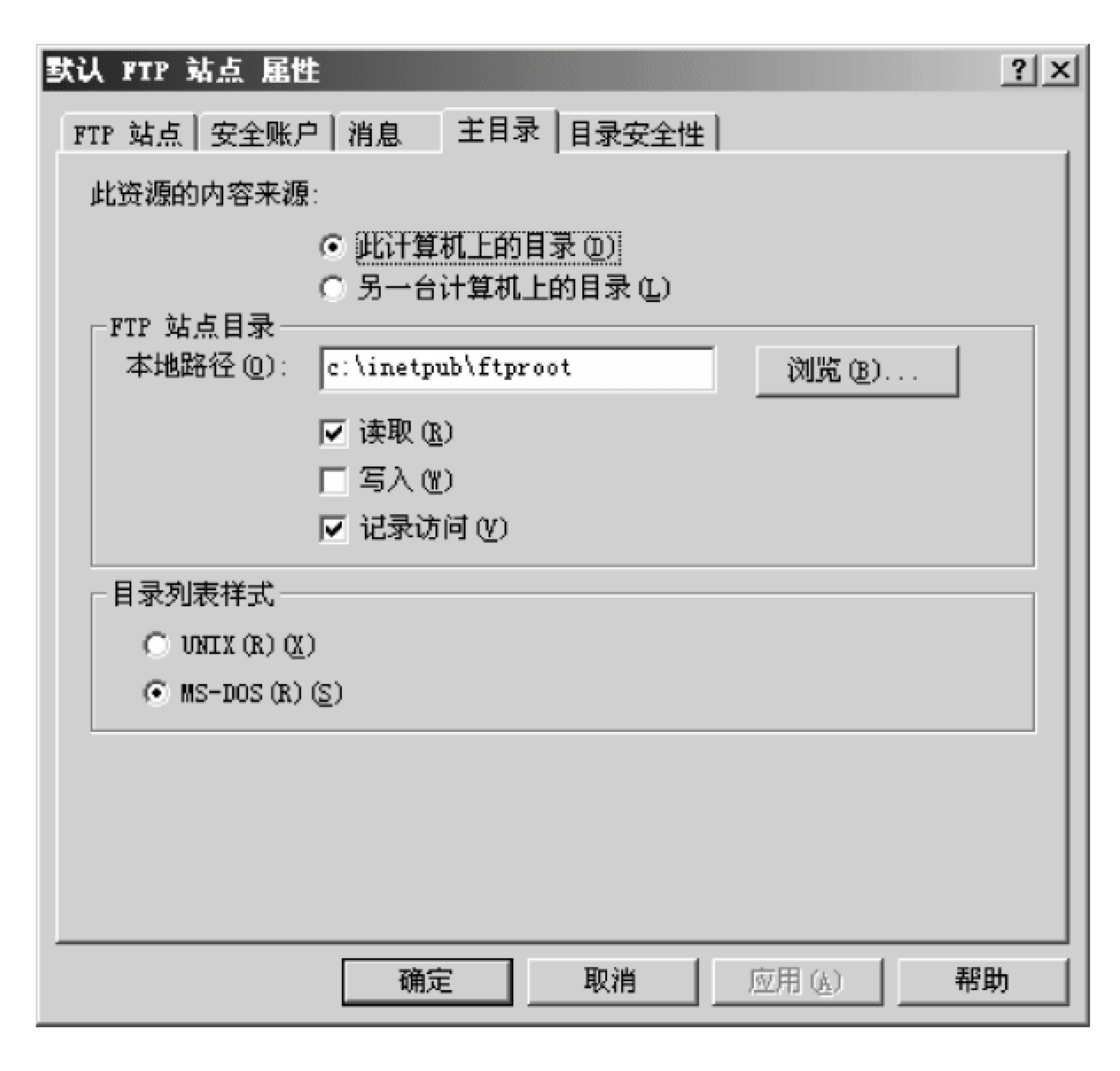


图 5-24 “主目录”选项卡

(8) 在“目录安全性”选项卡中对 FTP 服务器的访问控制权限进行分配,可通过此处将 FTP 服务器的访问权限授权给某部分 IP 用户或者拒绝来自某些 IP 用户的访问。注意,当选择了“授权访问”后,在下表中的 IP 地址将被拒绝,如果选择“拒绝访问”,下表中的 IP 地址用户将被授权。

2. 测试 FTP 服务器

FTP 服务器建立以后,可以通过下面方式对其进行测试:

(1) 打开“命令提示符”,在光标处输入 FTP 192.168.215.100;然后输入匿名账户 anonymous,密码为自己的邮件地址;接着就可通过 FTP 命令对 FTP 服务器进行操作。

(2) 通过 IE 来验证或者获取 FTP 服务,在 IE 的地址栏中输入 ftp://192.168.215.100/。

(3) 通过 FTP 客户端软件,如 FlashFTP、CuteFTP 等来访问 FTP 服务器。

3. 虚拟目录及多站点的配置

在 FTP 的配置过程中,经常需要对一个主机提供多个 FTP 站点来进行 FTP 共享。新站点的建立,可以通过新建站点向导一步步完成。形式上可通过一个主机上的不同 IP 地址来架设,或者通过同一个 IP 地址、不同的端口号来进行识别。如图 5-25 所示为使用同一 IP 地址、不同的端口号(2121)构建的第 2 个 FTP 站点。

在 FTP 的配置过程中,经常需要对多个不同路径的目录进行 FTP 共享,此时可通过虚拟目录来完成。虚拟目录是在主目录下通过某一个文件夹链接到其他目录的形式,在主目录中实际不存在此文件夹中的内容,该内容在其他目录下实际存在。新建虚拟目录可以通过新建虚拟目录向导完成,方法参考 5.5.1 节中 Web 服务器虚拟目录的建立。

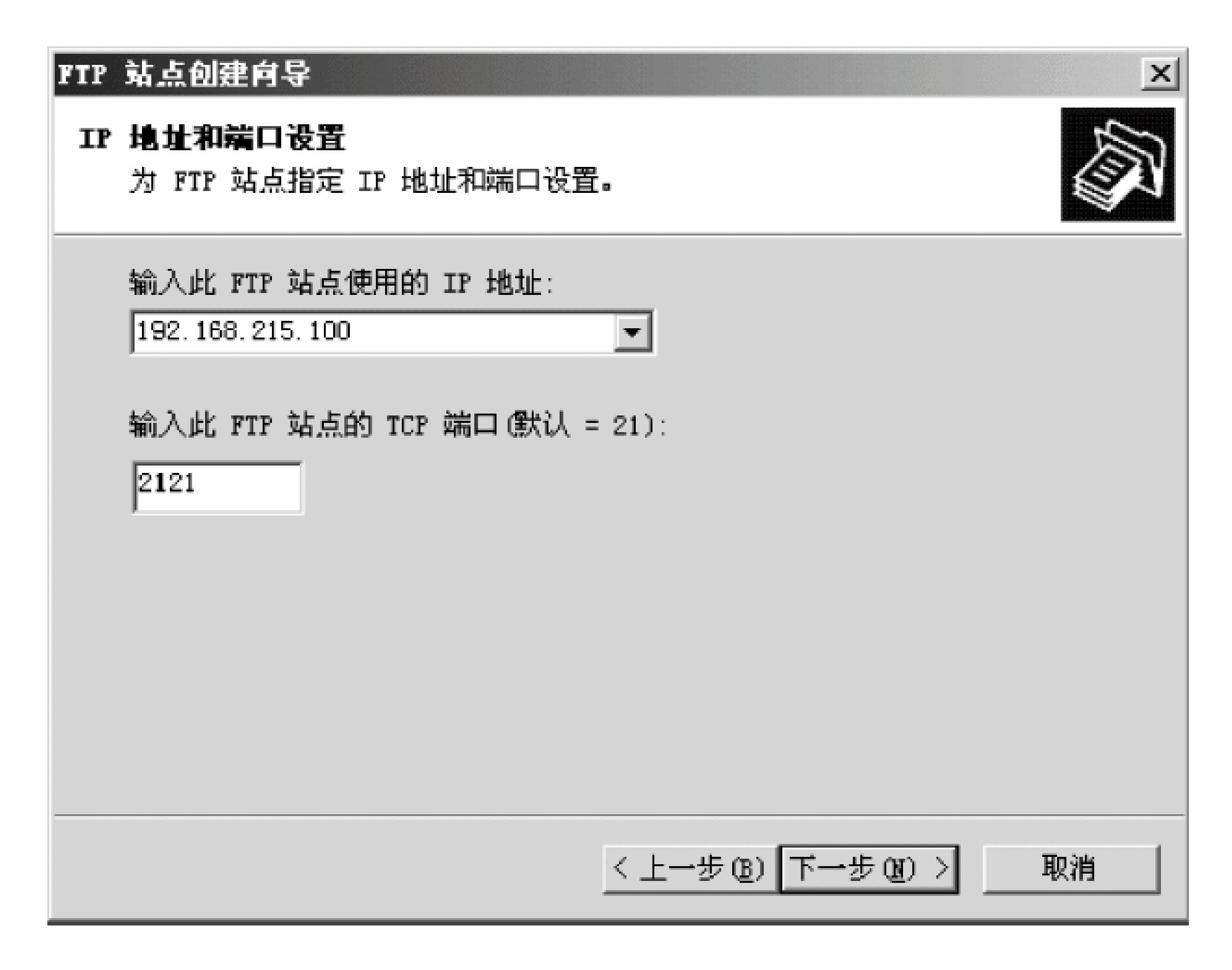


图 5-25　创建第 2 个 FTP 站点

5.1.5　接入服务器管理

1. 接入服务器简介

通过串行线路或调制解调器为远程终端、个人计算机提供网络连接，并向这些远程用户提供与其他的 LAN 或者 WAN 的连接的服务器称为接入服务器。接入服务器位于公用交换电话网与 IP 网的接口处，用户拨号通过交换机经用户线或中继线进入接入服务器。

接入服务器提供的服务一般有终端服务、远程交换服务、路由服务和协议转换服务等类型。网络接入服务器的功能组成可归类为 4 大功能模块。

(1) 接入功能模块：接入功能模块包括电话网侧的接口模块，分为 PSTN 的接口模块和 ISDN 的接口模块；还包括 IP 网侧的接口模块，包括 LAN 接口模块和同步专线接口模块；根据需要也可采用 FR 和 ATM 接口模块。

(2) 通信协议模块：接入服务器中包含众多通信协议，电话网侧通信协议(PPP)、IP 网侧通信协议(TCP/IP、UDP)、VPDN 协议等。

(3) 管理模块：接入服务器的管理模块包括 3 个子功能模块：SNMP 代理功能模块、Telnet 服务器功能模块和远端拨号监控功能模块。通过 3 种不同的途径对接入服务器进行控制管理。

(4) 接入认证、授权、计费和统计模块：接入服务器中包含网络接入认证与授权模块、计费模块和统计模块。

除了上述 4 类主要的功能模块外，还有一些其他的模块，诸如 VPDN 模块、来电指示模块和系统控制模块等。

2. 接入服务器的业务

(1) 中继合群业务

中继合群功能指接入服务器可以处理来自同一个中继群的不同被叫号(相应于不同的 ISP)的能力，中继合群适用于多个 ISP 共用同一接入服务器的情况，其功能为被叫号判别、

不同 IP 地址分配和不同接入认证系统的指向。接入服务器可以支持多种接入号码在同一中继群中接入，支持 PSTN 和 ISDN 用户在同一中继群中接入，并且接入号码相同。

目前，由中国电信经营和管理的比较大的网络 Chinanet 网和 Chinainfo 网，也就是 163 网络和 169 网络已经两网合一。那么如何实现不同 ISP 用户的接入呢？

当来自同一中继群的不同号码的呼叫进入接入服务器时，首先通过接入服务器强大的号码分析能力，将用户引入到不同 ISP 的认证系统，认证通过之后，系统根据不同的 ISP 号码分配给用户不同 IP POOL 中的地址，并通过源地址路由技术将用户引入不同的路由出口，从而访问 Internet。

(2) 多链路捆绑业务

多链路捆绑是 ML-PPP(Multilink-PPP)协议的核心技术，它是一个较为简单的协议。多链路捆绑可将多个物理链路捆绑成一个逻辑链路，扩展传输带宽；可对链路资源进行动态分配，有效地利用宝贵的带宽资源；解决了多径传输的时延问题，组网更加灵活。

ML-PPP 协议是通过对两个系统间同时存在的多条链路，分割、按序传送、重组 PPP 包的协议。在接入服务器内的 MP 捆绑包括 2 个 B 的捆绑和两个 Modem 的捆绑，以及一个 B 和一个 Modem 的捆绑等多种方式。接入服务器可以支持模拟-模拟链路捆绑、模拟-数字链路的捆绑、数字-数字链路捆绑、ISDN 的 30BB+D 链路捆绑。

(3) 回呼业务

随着社会的发展，在家中办公将逐渐成为时尚，与外界的连接往往通过互联网。员工平时在家里工作，当需要同企业总部进行联系或上网查找资料时，便可利用回呼功能上网，通过 Internet 进行办公。回呼功能使话费的承担者发生了变化，回呼用户只需承担开始一小段时间的话费，剩余话费记录在企业提供的账号上，由企业统一支付。

(4) VPDN 业务

Internet 的发展促使许多大型企业(如银行、铁路、公司等)内部网络实现了与 Internet 的互联。以往在政府部门之间、跨地区的企业内部网络之间的互联是通过专网实现的，这种接入方法极其昂贵，让大多数用户望而却步。而出差在外的人员如果需要与总部联系，往往需要通过拨号上网拨入企业内部网，这样又无法保证其安全性和可靠性。如何发挥互联网的效益，协助企业的发展是目前很多企业比较关注的问题。

VPDN(Virtual Private Dial Network)是 VPN 技术的一种，提供远程用户通过 PSTN/ISDN 拨号接入到 Internet，并建立隧道以传送数据至目的网络。VPDN 功能包括对请求建立虚拟数据专网的拨号用户进行用户资格认证，以及为通过资格认证的用户建立虚拟数据专网的隧道、数据包传送和拆除隧道等。接入服务器利用 VPN 技术可以实现多种新业务，企业只需在一个地方申请 VPN 业务，就可以在其他地方使用 VPN 业务。用户拨入当地的 ISP 接入服务器时，即使没有该地 ISP 账户也可享受相应服务。

(5) 端口批发业务

Internet 的飞速发展使得拨号接入网络的运营呈现前所未有的生机，但基于现有网络基础设施的投入和运营的规模效应之间存在比较大的差距，大多数 ISP 由于中继电路的昂贵和设备初期投入大而难以在短期内构建一个比较全面的拨号接入网络，并且投入所产生的规模效应难以实现，而大型网络运营商由于资金和现有的网络资源较有竞争力，逐渐与一些小型的 ISP 相分离，导致网络运营商致力于拨号网络的建设，而将部分网络资源(如拨号

端口)出租给 ISP、ICP 等,实现端口批发业务。

(6) IP 电话业务

IP 电话业务即是利用 Internet 网络作为传输通道并提供话音服务的一种业务。目前,IP 电话的发展潜力在于资费的低廉,随着电路交换向分组交换的演进,基于 IP 电话的增值业务呈现出了前所未有的生机,为 IP 电话运营商、ISP 等提供了更多的商机。通常的接入服务器是集程控交换、接入和 IP 电话于一体的多业务综合智能平台,在硬件不变的情形下,实现 IP 电话网关功能。

3. Windows Server 2003 的接入服务

Microsoft Windows Server 2003 中的“路由和远程访问”可以提供以下网络服务:

- 拨号远程访问服务器。
- 虚拟专用网络(VPN)远程访问服务器。
- 连接专用网络子网的 Internet 协议(IP)路由器。
- 将专用网络连接到 Internet 的网络地址转换器(NAT)。
- 拨号和 VPN 站点到站点请求拨号路由器。

“路由和远程访问”服务使远程用户可以通过 VPN 或拨号连接访问专用网络上的资源。“路由和远程访问”服务器可以提供 LAN 和 WAN 路由服务,用来连接小型办公网络中的网段或通过 Internet 连接两个专用网络。

通过将“路由和远程访问”配置为远程访问服务器,可以将远程工作人员或流动工作人员连接到相关组织的网络上。远程用户可以像其计算机物理连接到网络上一样进行工作,可以使用 LAN 中可用的所有服务(包括文件共享和打印机共享、Web 服务器访问和消息传递),如图 5-26 所示。

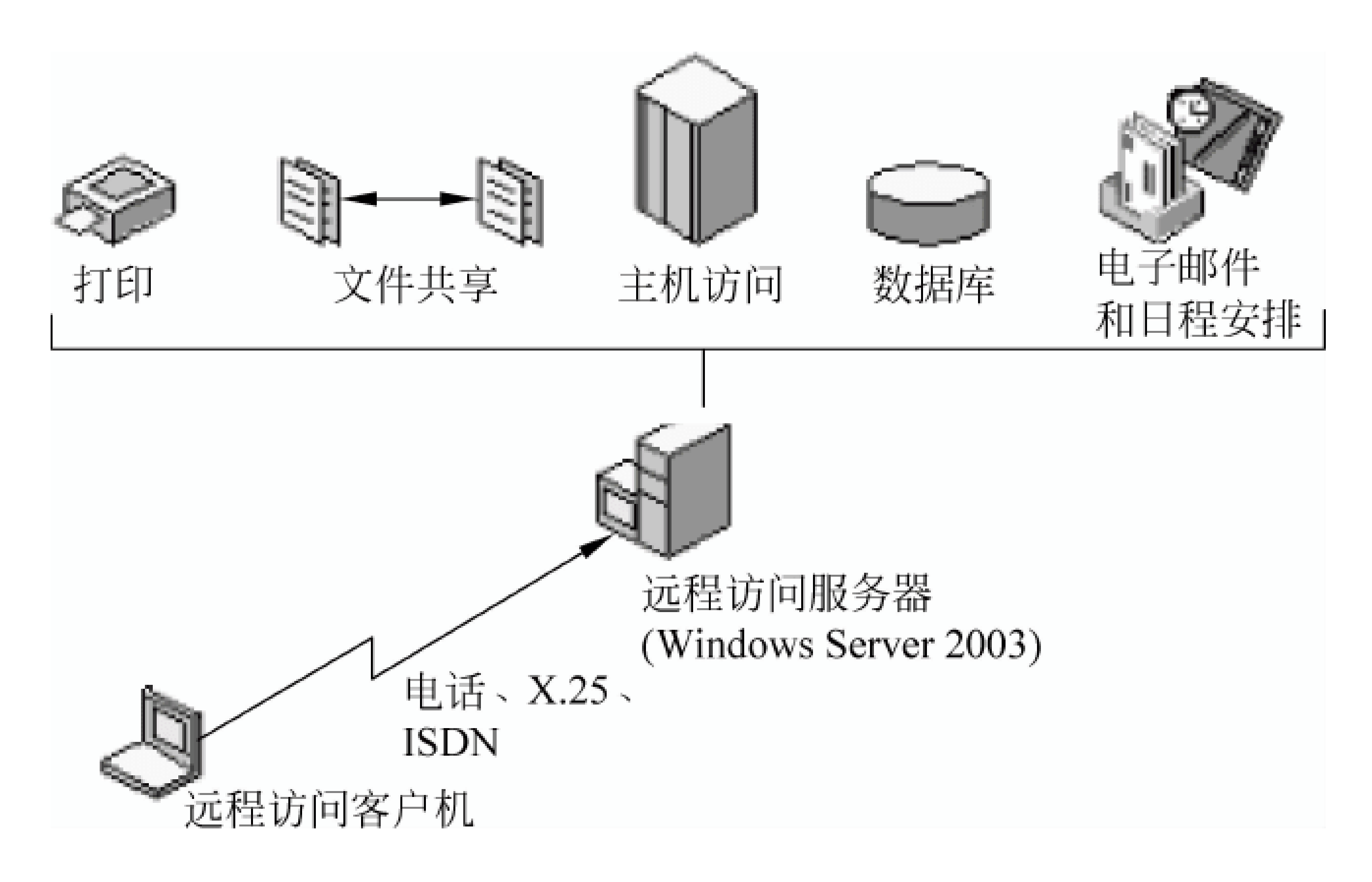


图 5-26 远程访问服务示意图

4. NAT 和 VPN 远程接入服务管理

NAT 和 VPN 的实现需要在服务器上安装双网卡,一块用于连接外网,一块接用于连接局域网。此外,需要安装 Windows Server 2003 中的“路由和远程访问”组件。

1) 开启 VPN 和 NAT 服务

(1) 依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”,然后打开“路由和远程访问”窗口;再在窗口左边右击本地计算机名,从快捷菜单中选择“配置并启用路由和远

程访问”，如图 5-27 所示。

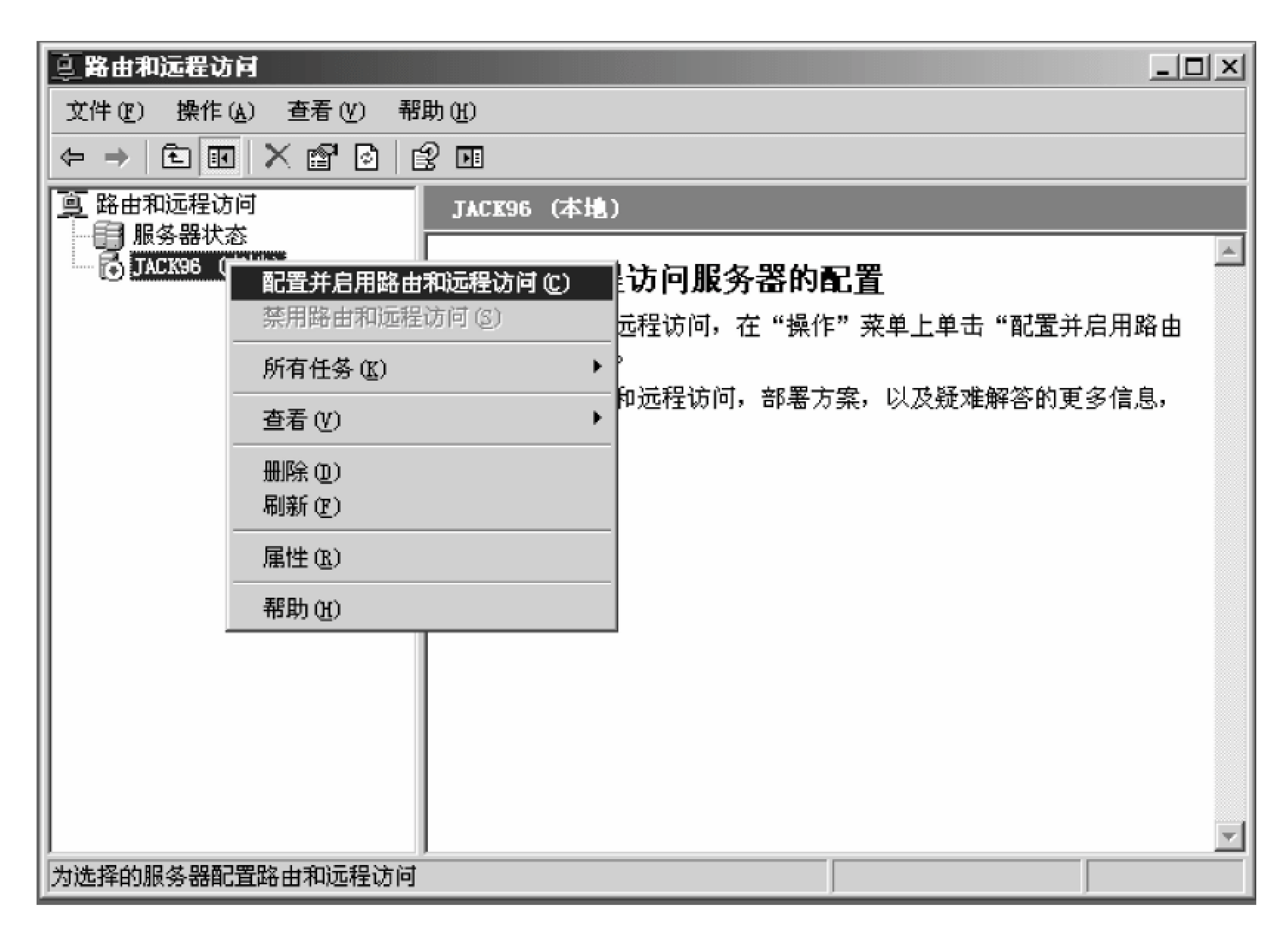


图 5-27 配置并启用路由和远程访问

(2) 在弹出的“路由和远程访问服务器安装向导”中单击“下一步”按钮，在出现的对话框中选择“自定义配置”选项，继续单击“下一步”按钮，出现如图 5-28 所示的对话框。



图 5-28 “自定义配置”对话框

这里选择“VPN 访问”和“NAT 和基本防火墙”复选框，然后单击“下一步”按钮，在弹出的对话框中单击“完成”按钮，系统会提示是否启动服务，单击“是”按钮，系统会按刚才的配置启动“路由和远程访问”服务，最终结果如图 5-29 所示。

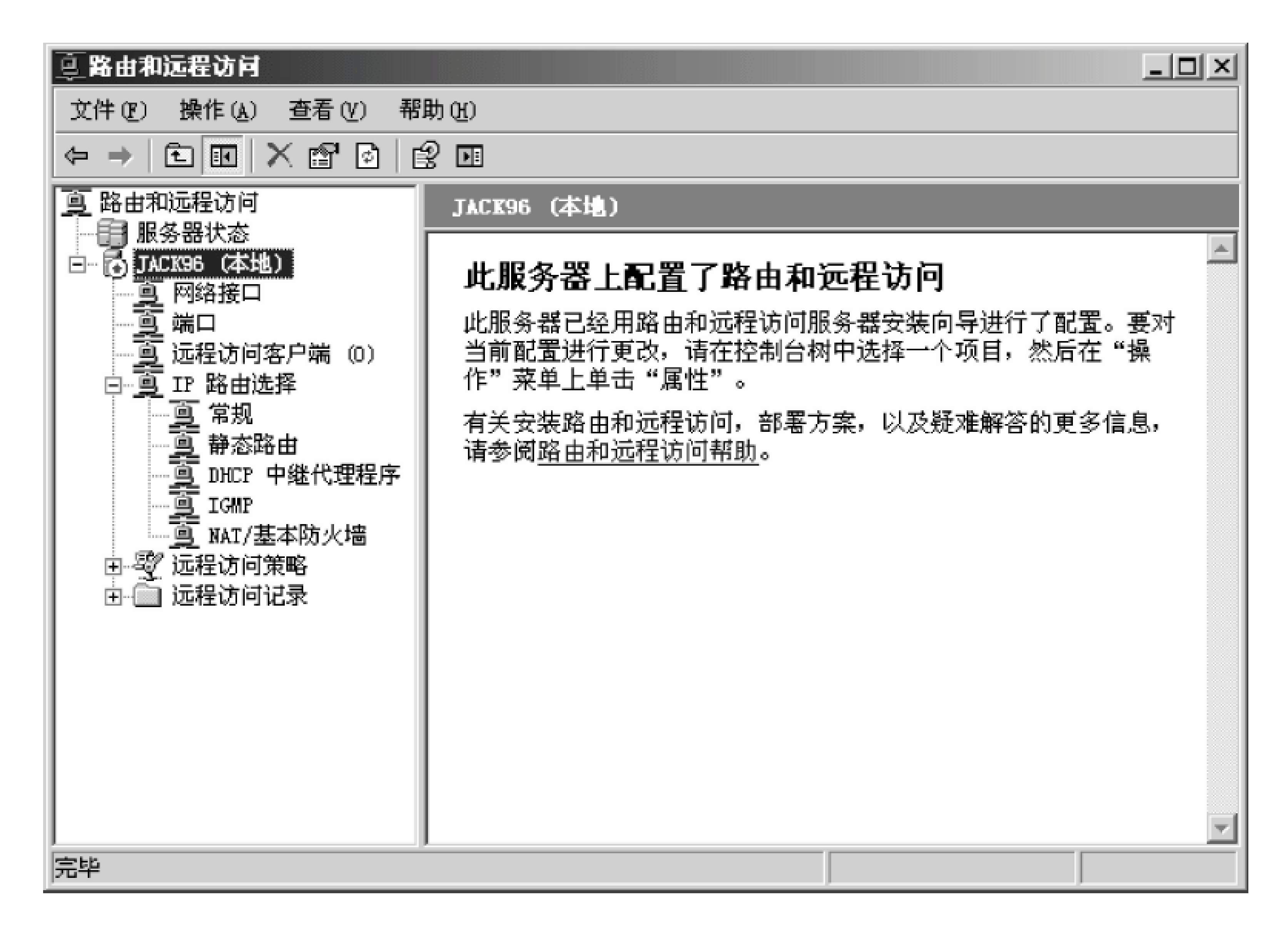


图 5-29　配置结果窗口

2）配置 NAT 服务

（1）在“路由和远程访问”窗口中右击“NAT/基本防火墙”选项，从快捷菜单中选择“新增接口”命令，在弹出的对话框中选择“wan”接口，单击“确定”按钮，弹出“网络地址转换-本地连接属性”对话框，进行如图 5-30 所示配置。

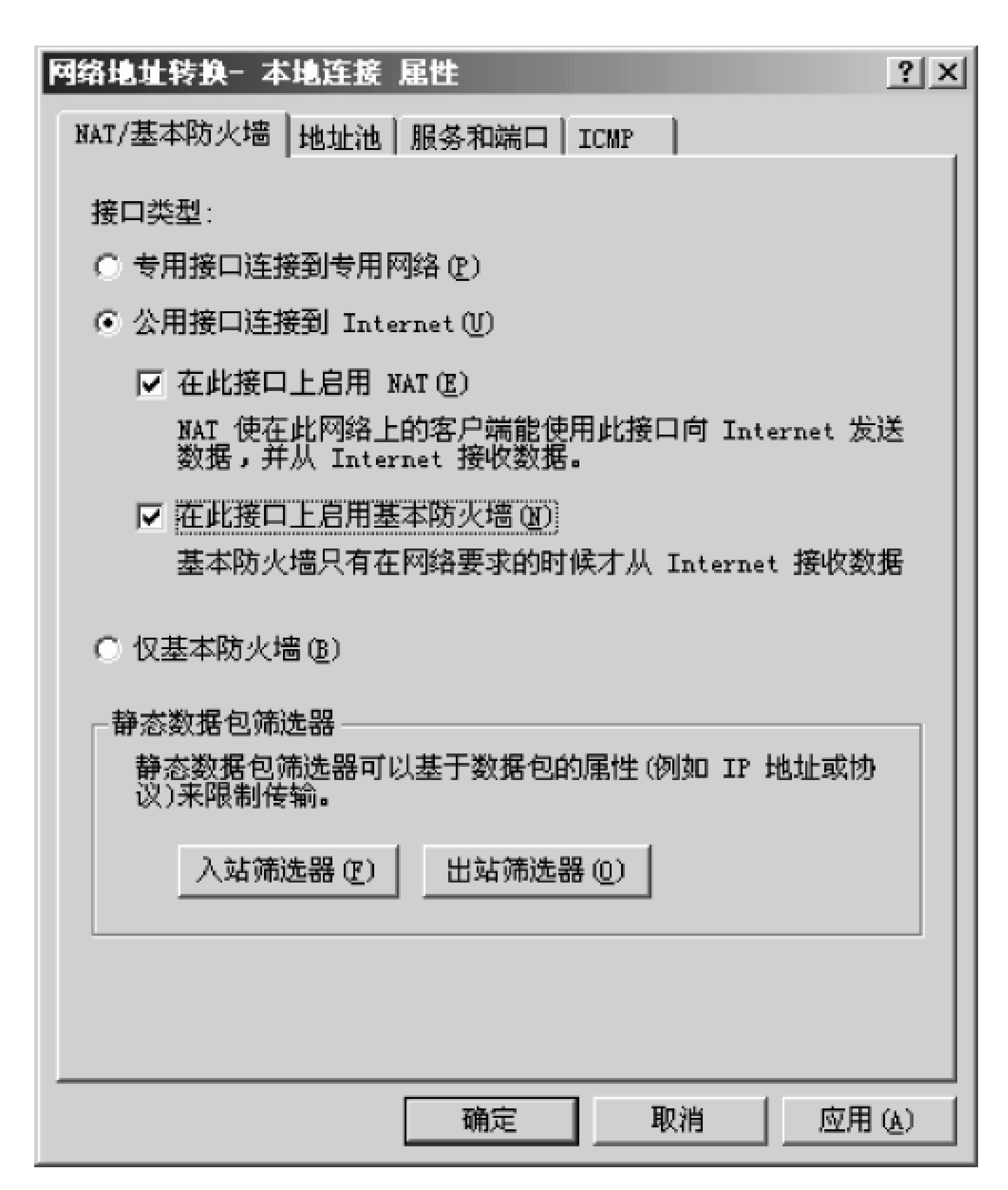


图 5-30　“NAT/基本防火墙”选项卡

由于这个网卡是连接外网的，所以选择“公用接口连接到 Internet”和“在此接口上启用 NAT”复选框，并选择“在此接口上启用基本防火墙”复选框，这对服务器的安全是非常重要的。

（2）单击“服务和端口”选项卡，设置服务器允许对外提供 PPTP VPN 服务，在“服务和

端口”选项卡中单击“VPN 网关(PPTP)”,在弹出的“编辑服务”对话框中进行如图 5-31 所示设置。

(3) 单击“确定”按钮,回到“服务和端口”选项卡,确保选中“VPN 网关(PPTP)”复选框,如图 5-32 所示。

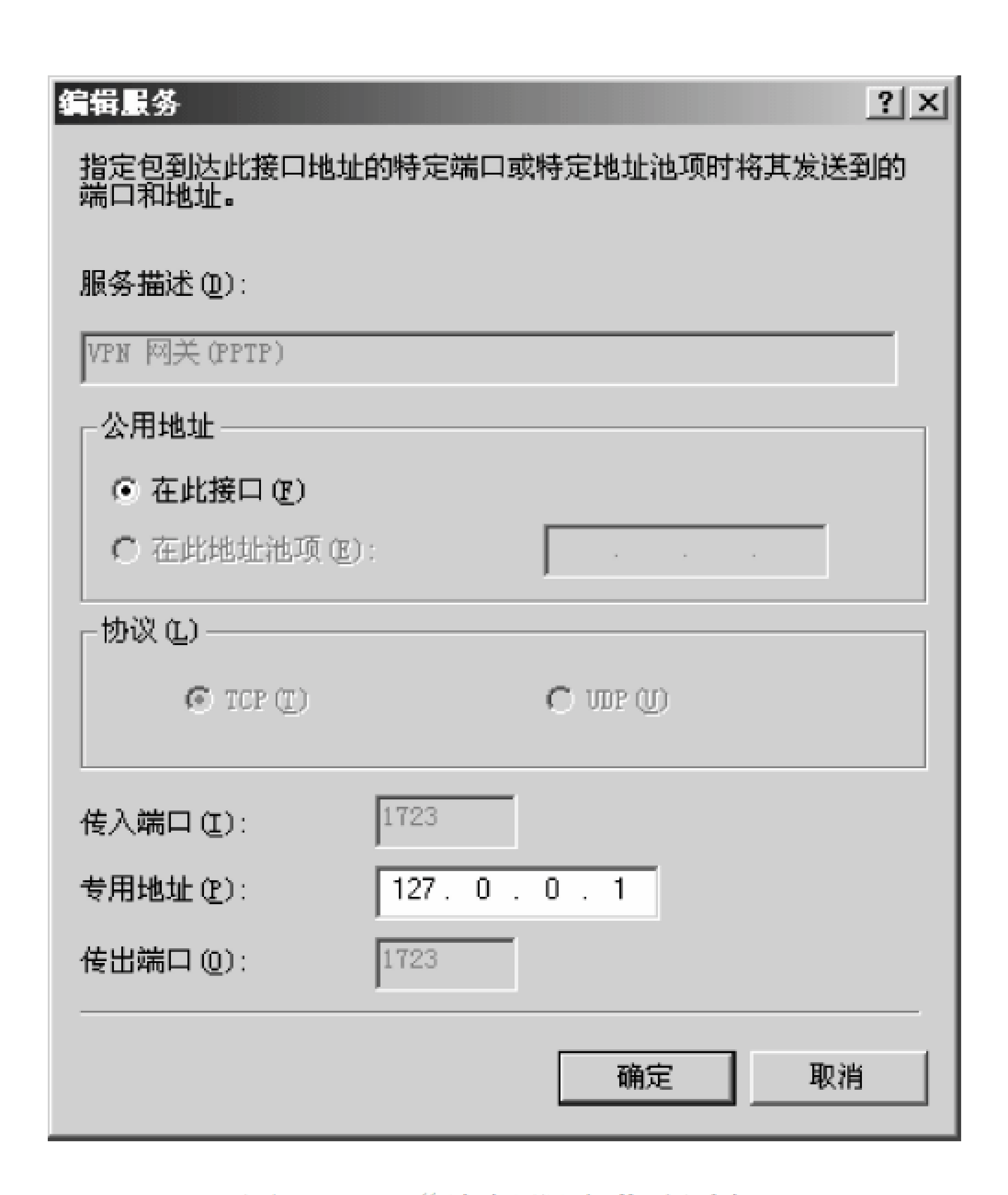


图 5-31 “编辑服务”对话框

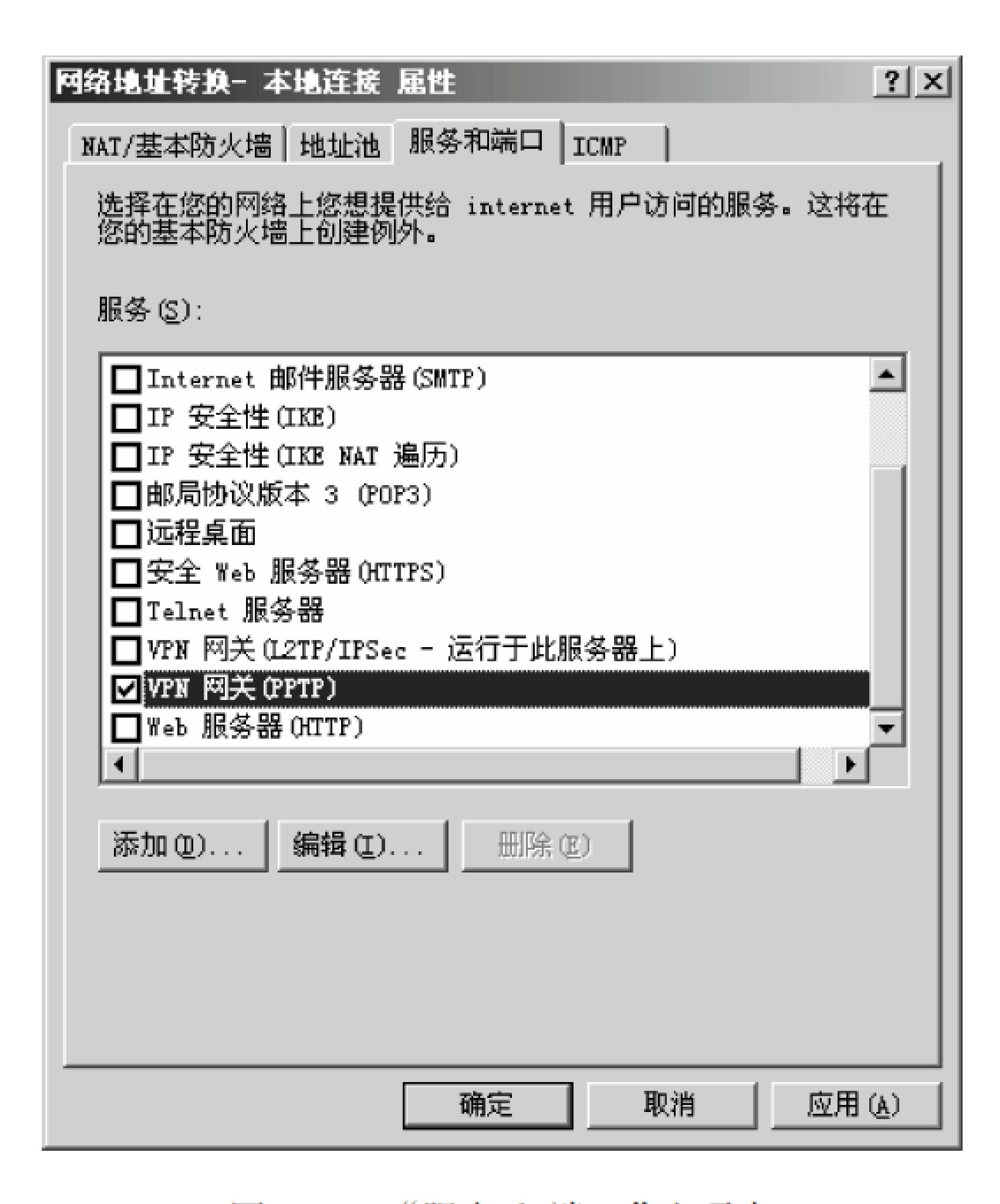


图 5-32 “服务和端口”选项卡

3) 设置 VPN 服务

(1) 设置连接数:右击“路由和远程访问”窗口中右边树型目录的“端口”选项,从快捷菜单中选择“属性”命令,弹出如图 5-33 所示的对话框。

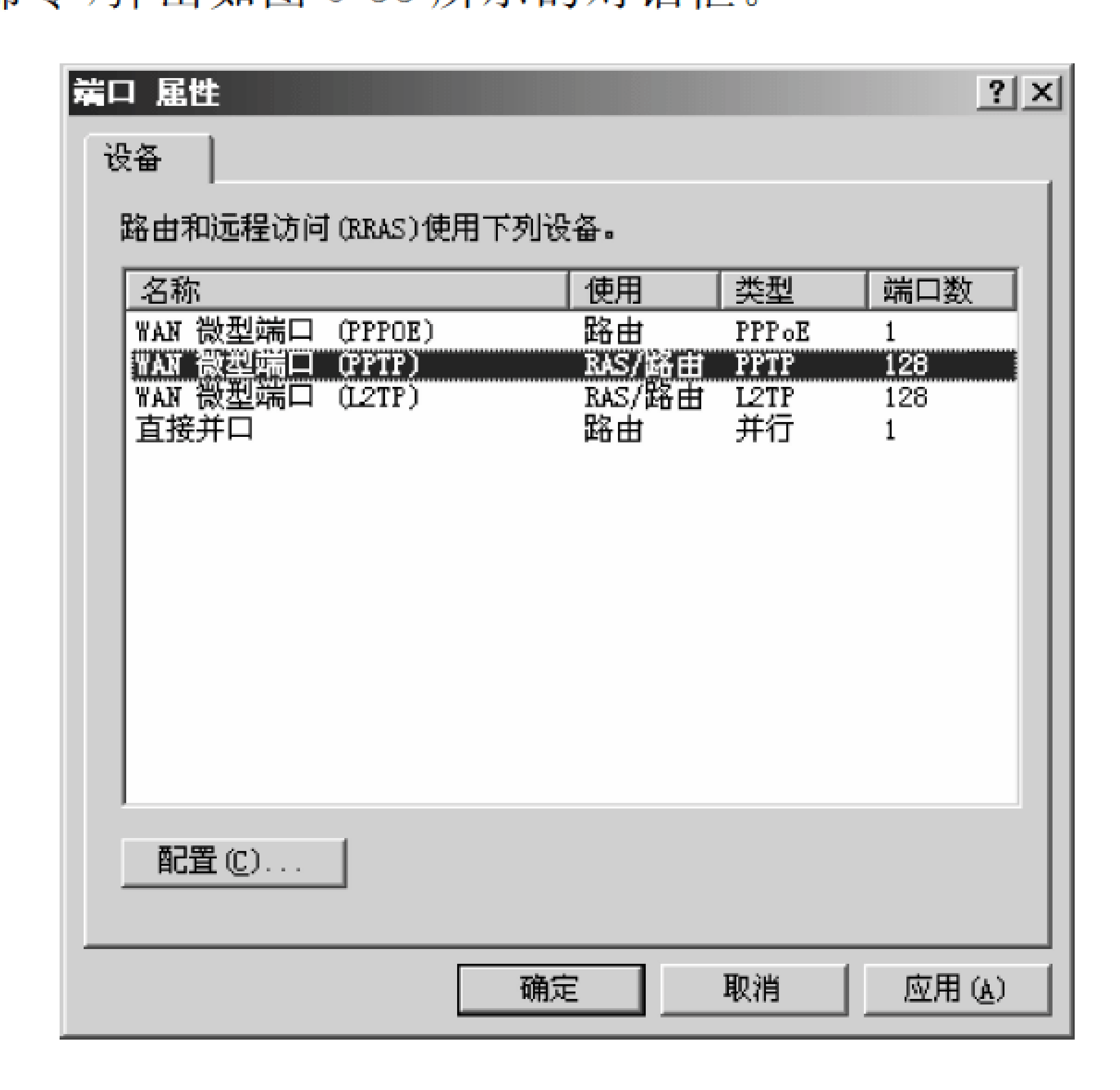


图 5-33 “端口属性”对话框

Windows Server 2003 企业版 VPN 服务默认支持 128 个 PPTP 连接和 128 个 L2TP 连接，因为要使用 PPTP 协议，所以双击"WAN 微型端口(PPTP)"选项，在弹出的如图 5-34 所示的对话框中，根据自己的需要设置所需的连接数。Windows Server 2003 企业版最多支持 30 000 个 L2TP 端口，16 384 个 PPTP 端口。

(2) 设置 IP 地址：在"路由和远程访问"窗口中右击树型目录里的本地服务器名，选择"属性"并切换到 IP 选项卡，如图 5-35 所示。

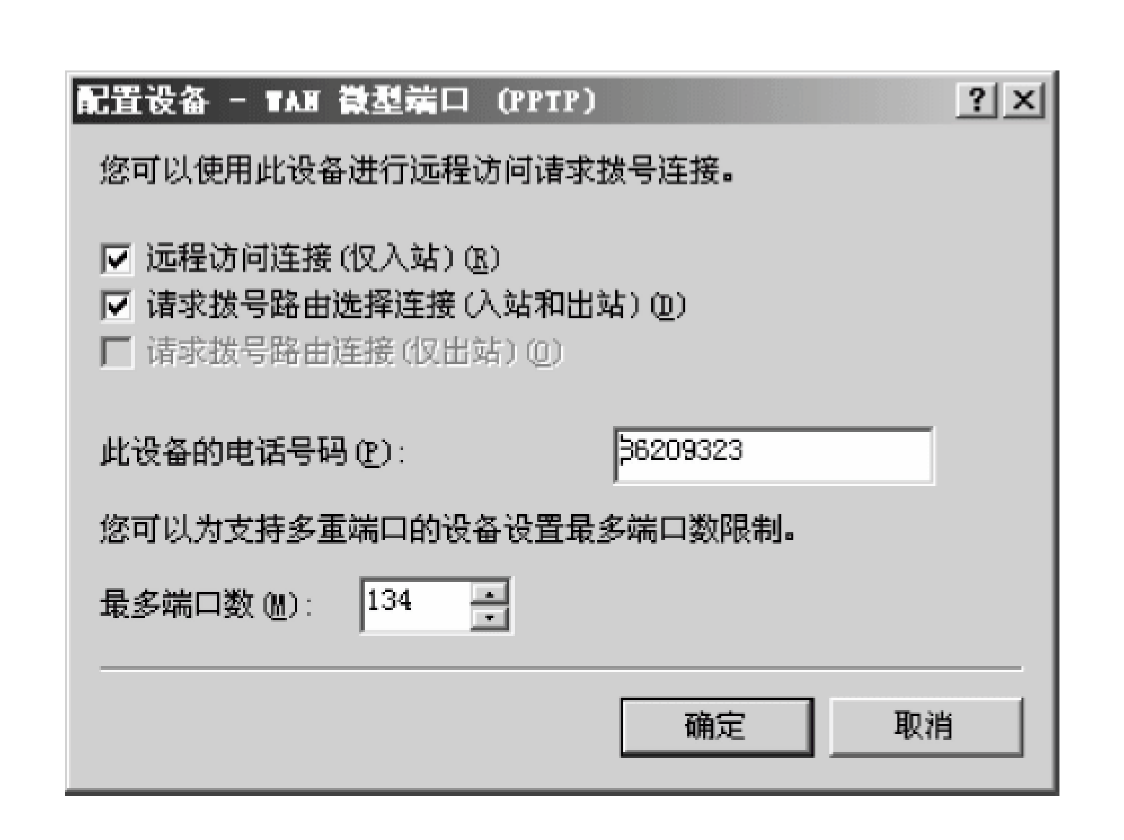


图 5-34　设置最多端口数

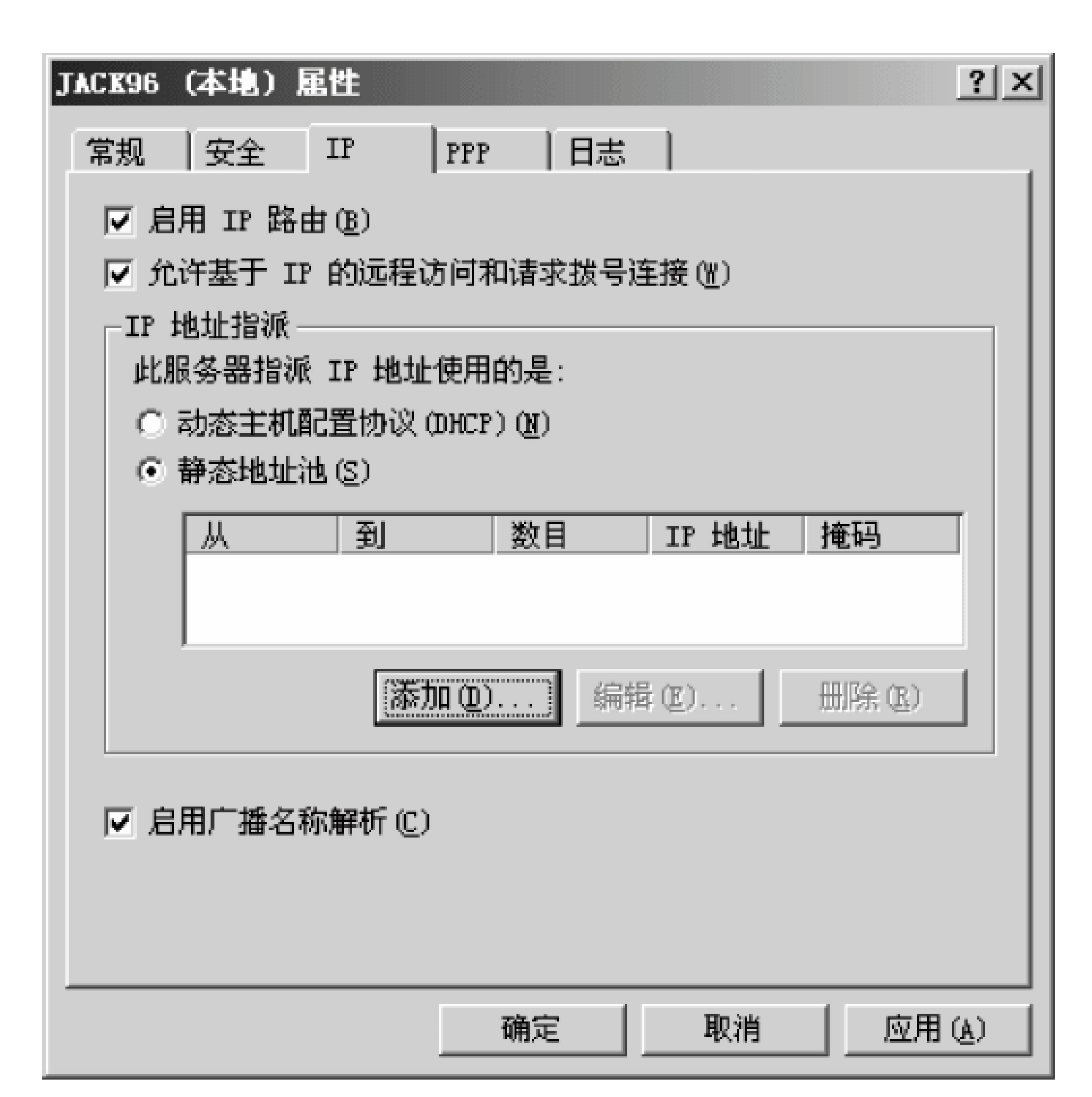


图 5-35　IP 选项卡

(3) 选择"静态地址池"后单击"添加"按钮，在弹出的"新建地址范围"对话框中，填写一个地址范围，但是不要和本地 IP 地址冲突。

(4) 单击"确定"按钮回到 IP 选项卡，继续单击"确定"按钮应用当前的设置。

4) 远程访问策略设置，允许指定用户拨入

(1) 新建用户和组：依次单击"开始"→"程序"→"管理工具"→"计算机管理"，在弹出的"计算机管理"对话框中选择"本地用户和组"，右击"用户"，从快捷菜单中选择"新用户"进行用户和用户组的创建。

(2) 设置远程访问策略：在"路由和远程访问"窗口中右击"远程访问策略"，从快捷菜单中选择"新建远程访问策略"，在弹出的对话框中单击"下一步"按钮，输入方便记忆的"策略名"，然后单击"下一步"按钮。

(3) 选择 VPN 选项，单击"添加"按钮把前面新建的组加入到这里，连续单击"下一步"按钮和"完成"按钮，完成远程策略的设置。

5) 配置 VPN 客户端

在客户端需要建立一个到 VPN 服务器端的专用连接，以 Windows XP 客户端为例建立 VPN 专用连接的方法如下：

(1) 在"网上邻居"图标单击鼠标右键并从快捷菜单中选择"属性"命令，然后单击"新建连接向导"打开向导窗口，然后单击"下一步"按钮；接着在"网络连接类型"窗口里选中"连

接到我的工作场所的网络”单选按钮，继续单击“下一步”按钮，在如图 5-36 所示的网络连接方式窗口里选择“虚拟专用网络连接”单选按钮；接着为此连接命名，然后单击“下一步”按钮。



图 5-36　网络连接方式设置

(2) 在确认公用网络已连接好的情况下，单击“下一步”按钮，在弹出的“VPN 服务器选择”窗口中，输入 VPN 服务端的主机名或 IP 地址；单击“下一步”按钮，为方便操作，可以选中“在桌面上建立快捷方式”选项，单击“完成”按钮即会先出现如图 5-37 所示的 VPN 连接对话框，输入合法的用户账号后即可访问 VPN 服务器。

(3) 共享操作。连接到服务器以后，可以通过“网上邻居”查找 VPN 服务端共享目录，也可以在浏览器里输入 VPN 服务端固定 IP 地址或动态域名，打开共享目录资源。这种操作就如同在局域网内的操作一样。



图 5-37　VPN 连接对话框

5.2 交换机管理

5.2.1 交换机的基本配置

交换是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术的统称。交换机就是一种在通信系统中完成信息交换功能的设备。

1. 二层交换机

二层交换机属数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。二层交换机的特性包括地址学习、转发与过滤以及避免循环等。二层交换机的工作过程如下：

(1) 当交换机从某个端口收到一个数据包后，它先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的。

(2) 再去读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

(3) 如表中有与这目的 MAC 地址对应的端口，把数据包直接复制到这个端口上。

(4) 如表中找不到相应的端口，则把数据包广播到所有端口上，当目的机器对源机器回应时，交换机又可以学习一目的 MAC 地址与哪个端口对应，在下次传送数据时就不再需要对所有端口进行广播了。

不断地循环这个过程，全网的 MAC 地址信息都可以被学习到，二层交换机就是这样建立和维护它自己的地址表的。

二层交换技术从网桥发展到 VLAN，在局域网建设和改造中得到了广泛的应用。第二层交换技术是工作在数据链路层，按照所接收到数据包的目的 MAC 地址来进行转发，对于网络层或者高层协议来说是透明的。它不处理网络层的 IP 地址，不处理高层协议的诸如 TCP、UDP 的端口地址，它只需要数据包的物理地址即 MAC 地址，数据交换是靠硬件来实现的，其速度相当快，这是二层交换的一个显著的优点。但是，它不能处理不同 IP 子网之间的数据交换。传统的路由器可以处理大量的跨越 IP 子网的数据包，但是它的转发效率比二层低，因此要想利用二层转发效率高这一优点，又要处理三层 IP 数据包，三层交换技术就诞生了。

2. 三层交换机

第三层交换工作在 OSI 七层网络模型中的第三层，即网络层。它利用第三层协议中的 IP 包的包头信息来对后续数据业务流进行标记，具有同一标记的业务流的后续报文被交换到第二层——数据链路层，从而打通源 IP 地址和目的 IP 地址之间的一条通路。这条通路经过第二层链路层，有了这条通路，三层交换机就没有必要每次将接收到的数据包进行拆包来判断路由，而是直接将数据包进行转发，将数据流进行交换。

一个具有三层交换功能的设备，是一个带有第三层路由功能的二层交换机，但它是二者的有机结合，并不是简单地把路由器设备的硬件及软件叠加在局域网交换机上。三层交换机的最重要目的是加快大型局域网内部的数据交换，所具有的路由功能也是为这目的服务的，能够做到一次路由，多次转发。对于数据包转发等规律性的过程由硬件高速实现，而像路由信息更新、路由表维护、路由计算、路由确定等功能，由软件实现。

3. 交换机管理的方式

可管理的交换机通常有超级终端方式、Telnet 方式和基于 Web 页面的管理方式。不过除了超级终端可以实现直接管理与远程管理外，Telnet 方式和 Web 页面方式都只适用于远程管理，并且必须借助于超级终端为设备指定 IP 地址、登录用户名和密码等可网管信息后才能实现。

1）超级终端方式

（1）线路连接设置

如图 5-38 所示，利用 Console 线将计算机的串口与交换机的 Console 端口连接在一起，可以通过计算机对交换机进行配置。

（2）“超级终端”设置

在计算机上需要安装一个终端仿真软件来登录网络设备，通常使用 Windows 自带的“超级终端”即可，超级终端的安装方法为：

依次单击“开始”→“程序”→“附件”→“通信”→“超级终端”，然后按照提示的步骤进行安装，其中连接的接口选择“COM1”，端口的速率选择“9600”，数据流控制选择“无”，其他都使用默认值。单击“确定”按钮后，可显示“超级终端”窗口。

接着，打开交换机的电源，连续按计算机的回车键即可显示交换机系统的初始化界面，并可以根据需要对交换机进行基本的设置。

（3）运行超级终端

在如图 5-39 所示的“连接到”对话框中的“连接时使用”下拉列表框中选择 TCP/IP（Winsock）选项，然后在“主机地址”文本框中输入欲配置和管理的远程交换机的管理 IP 地址，“端口号”通常采用默认值。

单击“确定”按钮后会显示登录页面，输入全局访问密码和 Enable 密码后即可进行相应的配置。



图 5-38　计算机与交换机 Console 端口的连接



图 5-39　“连接到”对话框

2）Telnet 方式

通过一台连接在网络中的计算机，用 Telnet 命令登录网络设备进行配置。

（1）远程登录条件

- 网络设备已经配置了 IP 地址、远程登录密码和特权密码。
- 网络设备已经连入网络工作。
- 计算机也连入网络，并且可以和网络设备通信。

(2) 远程登录方法

在计算机的命令行中，输入命令"telnet 网络设备 IP 地址"，输入登录密码就可以进入网络设备的命令配置模式。

3) Web 页面方式

有些交换机支持 Web 页面配置方式，可以通过浏览器访问交换机并进行配置，并可实时查看交换机的运行状态。通过 Web 浏览器的方式进行配置的方法如下：

(1) 把计算机连接在交换机的一个普通端口上，在计算机 Web 浏览器的"地址"栏中输入被管理交换机的 IP 地址或为其指定的名称。

(2) 分别在"用户名"和"密码"框中，输入拥有管理权限的用户名和密码。

(3) 单击"确定"按钮，即可建立与被管理交换机的连接，并在 Web 浏览器中显示交换机的管理界面。在该界面中输入超级用户的账号和密码后就可以通过 Web 界面中的提示，一步步查看交换机的各种参数和运行状态，并可根据需要对交换机的某些参数作必要的修改。

4) 其他方式

除了上述方式以外，还有其他一些配置交换机的方法，下面分别介绍。

(1) TFTP 服务器

TFTP 服务器是网络中的一台计算机，可以把网络设备的配置文件等信息备份到 TFTP 服务器之中，也可以把备份的文件传回到网络设备中。

由于设备的配置文件是文本文件，所以可以用文本编辑软件打开进行修改，再把修改后的配置文件传回网络设备，这样就可以实现配置功能。可以用 TFTP 服务器把一个已经做好的配置文件上传到一台同型号的设备中实现对它的配置。

(2) SSH

SSH 是一种安全的配置手段，其功能类似于远程登录。与 Telnet 不同的是，SSH 传输中所有信息都是加密的，所以如果需要在一个不能保证安全的环境中配置网络设备，最好使用 SSH。

4. 交换机的命令行(CLI)操作

(1) 命令模式

如表 5-1 所示，交换机的命令是按模式分组的，每种模式中定义了一组命令集，所以想要使用某个命令，必须先进入相应的模式。各种模式可通过命令提示符进行区分，命令提示符的格式是：提示符名 模式。

提示符名一般是设备的名字，交换机的默认名字是 Switch，路由器的默认名字是 Router，提示符模式表明了当前所处的模式。如：">"代表用户模式，"#"代表特权模式。

表 5-1 交换机的命令模式

模　式	提 示 符	说　明
User EXEC(用户模式)	>	用于查看系统基本信息和进行基本测试
Privileged EXEC(特权模式)	#	查看、保存系统信息
Global configuration(全局配置模式)	(config)#	配置设备的全局参数
Interface configuration(接口配置模式)	(config-if)#	配置设备的各种接口
Line configuration(线路配置模式)	(config-line)#	配置控制台、远程登录等线路
Config-vlan(VLAN 配置模式)	(config-vlan)#	配置 VLAN 参数

（2）命令模式的切换

交换机的模式大体可分为四层：用户模式→特权模式→全局配置模式→其他配置模式。进入某模式时，需要逐层进入，模式切换的命令如表 5-2 所示。

表 5-2　命令模式的切换命令

要　　求	命 令 举 例	说　　明
进入用户模式		登录后就进入
进入特权模式	Switch>enable	在用户模式中输入 enable 命令
进入全局配置模式	Switch# configure terminal	在特权模式中输入 conf t 命令
进入接口配置模式	Switch(config)# interface f0/1	在全局配置模式中输入 interface 命令，该命令可带不同参数
进入线路配置模式	Switch(config)# line console 0	在全局配置模式中输入 line 命令，该命令可带不同参数
进入 VLAN 配置模式	Switch(config)# vlan 3	在全局配置模式中输入 vlan 命令，该命令可带不同参数
退回到上一层模式	Switch(config-if)# exit	用 exit 命令可退回到上一层模式
退回到特权模式	Switch(config-if)# end	用 end 命令或按 Ctrl+Z 快捷键可从各种配置模式中直接退回到特权模式
退回到用户模式	Switch# disable	从特权模式退回到用户模式

5. 交换机的配置

以 Cisco 的交换机为例，Cisco 的交换机产品以 Catalyst 为商标，包含 1900、2800、2900、3500、4000、5000、5500、6000、8500 等十多个系列。总的来说，这些交换机可以分为两类：一类是固定配置交换机，包括 3500 及以下的大部分机型，除了有限的软件升级之外，这些交换机不能扩展；另一类是模块化交换机，主要指 4000 及以上的机型，用户可以根据网络的需求，选择不同数目和型号的接口板、电源模块及相应的软件。Catalyst 交换机基本配置命令如下：

（1）设置主机名/系统名

```
!在基于 IOS 的交换机上设置主机名/系统名
switch(config)#  hostname hostname
!在基于 CLI 的交换机上设置主机名/系统名
switch(enable) set system name name-string
```

（2）设置登录口令

```
!在基于 IOS 的交换机上设置登录口令
switch(config)#  enable password level 1 password
!在基于 CLI 的交换机上设置登录口令
switch(enable) set password
switch(enable) set enablepass
```

（3）设置远程访问

```
!在基于 IOS 的交换机上设置远程访问
switch(config)#  interface vlan 1
switch(config-if)#  ip address ip-address netmask
```

switch(config-if)# ip default-gateway *ip-address*
!在基于 CLI 的交换机上设置远程访问:
switch(enable) set interface sc0 *ip-address netmask broadcast-address*
switch(enable) set interface sc0 vlan
switch(enable) set ip route *default gateway*

(4) 浏览 CDP 信息

!在基于 IOS 的交换机上启用和浏览 CDP 信息
switch(config-if)# cdp *enable*
switch(config-if)# no cdp *enable*
!查看 Cisco 邻接设备的 CDP 通告信息
switch# show cdp interface [type module/port]
switch# show cdp neighbors [type module/port] [detail]
!在基于 CLI 的交换机上启用和浏览 CDP 信息
switch(enable) set cdp {enable|disable} module/port
!查看 Cisco 邻接设备的 CDP 通告信息
switch(enable) show cdp neighbors[module/port] [vlan|duplex|capabilities|detail]

(5) 端口描述

!基于 IOS 的交换机的端口描述
switch(config-if)# description des *cription-string*
!基于 CLI 的交换机的端口描述
switch(enable)set port name *module/number des cription-string*

(6) 设置端口速度

!在基于 IOS 的交换机上设置端口速度
switch(config-if)# speed{10|100|auto}
!在基于 CLI 的交换机上设置端口速度
switch(enable) set port speed *module/number* {10|100|auto}
switch(enable) set port speed *module/number* {4|16|auto}

(7) 设置以太网的链路模式

!在基于 IOS 的交换机上设置以太网的链路模式
switch(config-if)# duplex {auto|full|half}
!在基于 CLI 的交换机上设置以太网的链路模式
switch(enable) set port duplex *module/number* {full|half}

(8) 配置静态 VLAN

!在基于 IOS 的交换机上配置静态 VLAN
switch# vlan database
switch(vlan)# vlan *vlan-num* name *vlan*
!在基于 CLI 的交换机上配置静态 VLAN
switch(enable) set vlan *vlan-num* [name name]
switch(enable) set vlan *vlan-num mod-num/port-list*

5.2.2 VLAN 管理

1. VLAN 的概念

VLAN 可以不考虑用户的物理位置,而根据功能、应用等因素将用户从逻辑上划分为

一个个功能相对独立的工作组，每个用户主机都连接在一个支持 VLAN 的交换机端口上并属于一个 VLAN。一个 VLAN＝一个广播域＝一个逻辑网段（子网），同一个 VLAN 中的成员都共享广播，形成一个广播域，而不同 VLAN 之间广播信息是相互隔离的。

一般来说，如果一个 VLAN 里面的工作站发送一个广播，那么这个 VLAN 里面所有的工作站都会接收到这个广播，但是交换机不会将广播发送至其他 VLAN 上的任何一个端口。如果要将广播发送到其他的 VLAN 端口，就要用到三层交换机。当然，VLAN 也可以在不同的交换机中实现，跨交换机的 VLAN 的通信要通过 TRUNK 实现。

2. VLAN 的类型

Cisco 交换机 VLAN 的实现通常是以端口为中心的，将端口分配给 VLAN 有静态和动态两种方式。

（1）静态方式：将端口强制性地分配给 VLAN。即先在 VTP（VLAN Trunking Protocol）Server 上建立 VLAN，然后将每个端口分配给相应的 VLAN 的过程。

（2）动态方式：动态方式由端口决定自己属于哪个 VLAN。即先建立一个 VLAN 管理策略服务器（VLAN Membership Policy Server，VMPS），VMPS 里面包含一个文本文件，文件中存有与 VLAN 映射的 MAC 地址表，交换机根据这个映射表决定将端口分配给哪个 VLAN。

3. VLAN 的配置

下面以实例介绍创建 VLAN 的命令和 VLAN 实现的过程。假设某局域网由一台具备三层交换功能的核心交换机和几台分支交换机（不一定具备三层交换功能）组成。核心交换机名称为 CORE；分支交换机分别为：S1、S2、S3、…，VLAN 名称分别为 COUNT、MARKET、MANAGE…。

1）设置 VTP DOMAIN

VTP DOMAIN 称为管理域，交换 VTP 更新信息的所有交换机必须配置为相同的管理域。如果所有的交换机都以中继线相连，那么只要在核心交换机上设置一个管理域，网络上所有的交换机都加入该域，这样管理域里所有的交换机就能够了解彼此的 VLAN 列表。

```
CORE# vlan database                 !进入 VLAN 配置模式
CORE(vlan)# vtp domain CORE         !设置 VTP 管理域名称 CORE
CORE(vlan)# vtp Server              !设置交换机为服务器模式
S1# vlan database
S1(vlan)# vtp domain CORE
S1(vlan)# vtp Client                !设置交换机为客户端模式
S2# vlan database
S2(vlan)# vtp domain CORE
S2(vlan)# vtp Client
S3# vlan database
S3(vlan)# vtp domain CORE
S3(vlan)# vtp Client
```

交换机设置为 Server 模式是指允许在本交换机上创建、修改、删除 VLAN 及其他一些对整个 VTP 域的配置参数，同步本 VTP 域中其他交换机传递来的最新的 VLAN 信息；Client 模式是指本交换机不能创建、删除、修改 VLAN 配置，也不能在 NVRAM 中存储 VLAN 配置，但可以同步由本 VTP 域中其他交换机传递来的 VLAN 信息。

2）配置中继

为了保证管理域能够覆盖所有的分支交换机，必须配置中继。Cisco 交换机能够支持任何介质作为中继线，为了实现中继可使用其特有的 ISL 标签。ISL（Inter-Switch Link）是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，通过在交换机直接相连的端口配置 ISL 封装，即可跨越交换机进行整个网络的 VLAN 分配和配置。

在核心交换机端配置如下：

```
CORE(config)#interface gigabitEthernet 2/1
CORE(config-if)#switchport                !把端口设置为 2 层模式
CORE(config-if)#switchport trunk encapsulation isl
CORE(config-if)#switchport mode trunk
CORE(config)#interface gigabitEthernet 2/2
CORE(config-if)#switchport
CORE(config-if)#switchport trunk encapsulation isl
CORE(config-if)#switchport mode trunk
CORE(config)#interface gigabitEthernet 2/3
CORE(config-if)#switchport
CORE(config-if)#switchport trunk encapsulation isl
CORE(config-if)#switchport mode trunk
```

在分支交换机端配置如下：

```
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode trunk
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#switchport mode trunk
S3(config)#interface gigabitEthernet 0/1
S3(config-if)#switchport mode trunk
……
```

3）创建 VLAN

一旦建立了管理域，就可以创建 VLAN 了，下面创建编号分别为 10、11、12 的 VLAN：

```
CORE(vlan)#Vlan 10 name COUNT !创建了一个编号为 10 名字为 COUNT 的 VLAN
CORE(vlan)#Vlan 11 name MARKET
CORE(vlan)#Vlan 12 name MANAGE
```

这里的 VLAN 是在核心交换机上建立的，其实只要是在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN，它就会通过 VTP 通告整个管理域中的所有的交换机。但是如果要将交换机的端口划入某个 VLAN，就必须在该端口所属的交换机上进行设置。

4）将交换机端口划入 VLAN

要将 S1、S2、S3…分支交换机的端口 1 划入 COUNT，端口 2 划入 MARKET，端口 3 划入 MANAGE，配置如下：

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport access vlan 10
```

```
S1(config)#interface fastEthernet 0/2
S1(config-if)#switchport access vlan 11
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport access vlan 12
……
```

至此,VLAN 已经基本划分完毕,但 VLAN 间尚不能实现三层交换,还需要给各 VLAN 分配 IP 地址。

5)配置三层交换

假设 COUNT 的 IP 地址为 172.16.10.1/24,网络地址为:172.16.10.0;MARKET 的 IP 地址为 172.16.20.1/24,网络地址为 172.16.20.0;MANAGE 的 IP 地址为 172.16.30.1/24,网络地址为 172.16.30.0。如果动态分配 IP 地址,则设网络上的 DHCP 服务器 IP 地址为 172.16.1.55。

(1)给 VLAN 所有的节点分配静态 IP 地址

首先在核心交换机上分别设置各 VLAN 的接口 IP 地址,方法为:

```
rCORE(config)#interface vlan 10
CORE(config-if)#ip address 172.16.10.1 255.255.255.0 !VLAN10 接口 IP
COM(config)#interface vlan 11
CORE(config-if)#ip address 172.16.20.1 255.255.255.0 !VLAN11 接口 IP
CORE(config)#interface vlan 12
CORE(config-if)#ip address 172.16.30.1 255.255.255.0 !VLAN12 接口 IP
……
```

再在各接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址,并且把默认网关设置为该 VLAN 的接口地址。这样,所有的 VLAN 也可以互访了。

(2)给 VLAN 所有的节点分配动态 IP 地址

首先在核心交换机上分别设置各 VLAN 的接口 IP 地址和 DHCP 服务器的 IP 地址,方法为:

```
CORE(config)#interface vlan 10
CORE(config-if)#ip address 172.16.10.1 255.255.255.0      !vlan 10 接口 IP
CORE(config-if)#ip helper-address 172.16.1.55             !DHCP Server IP
CORE(config)#interface vlan 11
CORE(config-if)#ip address 172.16.20.1 255.255.255.0      !vlan 11 接口 IP
CORE(config-if)#ip helper-address 172.16.1.55             !DHCP Server IP
CORE(config)#interface vlan 12
CORE(config-if)#ip address 172.16.30.1 255.255.255.0      !vlan 12 接口 IP
CORE(config-if)#ip helper-address 172.16.1.55             !DHCP Server IP
```

再在 DHCP 服务器上设置网络地址分别为 172.16.10.0,172.16.20.0,172.16.30.0 的作用域,并将这些作用域的“路由器”选项设置为对应 VLAN 的接口 IP 地址。这样,可以保证所有的 VLAN 也可以互访了。

最后在各接入 VLAN 的计算机中进行网络设置,将 IP 地址选项设置为自动获得 IP 地址即可。

5.3 路由器管理

5.3.1 路由器的基本配置

1. 路由器的概念

路由器是连接 Internet 中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径按前后顺序发送信号。路由的传递依赖于路由表，路由表的构建是由路由器中运行的路由协议完成的。常见的路由协议有 RIP、IGRP、OSPF 和 EIGRP 等。

路由器根据自己的路由表来选择到达目标 IP 地址的最佳路径出口，然后重定向数据包第二层的帧头，让数据包发往下一跳，最终将数据发送到目的地。路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、背板转发以及输出链路调度等。控制功能包括与相邻路由器间的信息交换、系统配置和系统管理等。

2. 路由器的组成与启动过程

1）路由器的组成

与计算机相似，路由器也是由硬件系统和软件系统两部分组成的。硬件系统主要由中央处理器、内存、接口以及控制台端口等物理硬件和电路组成；而软件系统则主要由路由器的 IOS 操作系统构成。与计算机不同，路由器的内存由 RAM、ROM、FLASH 和 NVRAM 组成。

- RAM（随机访问存储器）：RAM 中运行着 Cisco IOS 的镜像文件以及 running-config 文件。
- ROM（只读存储器）：ROM 中保存着最基本功能的代码，用于引导路由器。
- FLASH（闪存）：一种可擦写、可编程的存储器，相当于计算机的硬盘。FLASH 中容纳了 IOS 软件的镜像文件。
- NVRAM（非易失性随机访问存储器）：NVRAM 用来存储 startup-config 文件，当切断电源时，NVRAM 用一个电池来维护其中的数据。

2）启动过程

路由器启动过程可以分为以下几步：

（1）POST（加电自检），检测路由器的硬件。

（2）装载 ROM 中的 Bootstrap 代码：这里的 Bootstrap 代码与 PC 的 BIOS 相似，用于初始化时启动路由器。路由器在此读取配置寄存器的内容以决定后面的操作。

（3）查找 IOS：一般情况下，IOS 放在闪存中，Bootstrap 会告诉路由器放在哪里，如果闪存中存在多个镜像文件，还要由 NVRAM 中的配置文件来决定加载哪个镜像文件。

（4）装载 IOS：将 IOS 装载到内存中，或者在闪存中直接加载。

（5）寻找配置文件：配置文件一般保存在 NVRAM 中。有时候，用户可以将路由器设置为从 TFTP 服务器寻找配置文件。

（6）装载配置，最后正常运行。

3. 路由器的命令

1）路由器的命令模式

路由器的命令模式与交换机的命令模式相似，如表 5-3 所示。

表 5-3　路由器的命令模式

模式类型	命令提示符	功能说明	访问方法	退出方法
用户模式	>	执行基本测试、显示系统信息		logout/quit
特权用户模式	#	校验输入的命令	enble	disable
全局配置模式	(config)#	将配置的参数应用于整个路由器	config terminal	exit/^z
端口配置模式	(config-if)#	配置端口	interface	exit/end/^z
虚拟局域网模式	(config-vlan)#	配置 vlan	vlan	exit/end/^z
进程配置模式	(config-line)#	为 line 模式管理配置参数	line vty	exit/end/^z

2）路由器的常用命令

(1) 帮助

在 IOS 操作中，无论任何状态和位置，都可以输入“?”得到系统的帮助。

(2) 改变命令状态

改变命令状态的常用命令如表 5-4 所示。

表 5-4　改变命令状态命令表

任务	命令
进入特权命令状态	enable
退出特权命令状态	disable
进入设置对话状态	setup
进入全局设置状态	config terminal
退出全局设置状态	end
进入端口设置状态	interface *type slot/number*
进入子端口设置状态	interface *type number.subinterface* [point-to-point ｜ multipoint]
进入线路设置状态	line *type slot/number*
进入路由设置状态	router *protocol*
退出局部设置状态	exit

(3) 显示命令(见表 5-5)

表 5-5　显示命令表

任务	命令
查看版本及引导信息	show version
查看运行设置	show running-config
查看开机设置	show startup-config
显示端口信息	show interface *type slot/number*
显示路由信息	show ip router

(4) 拷贝命令

用于 IOS 及 CONFIG 的备份和升级，拷贝命令功能如图 5-40 所示。

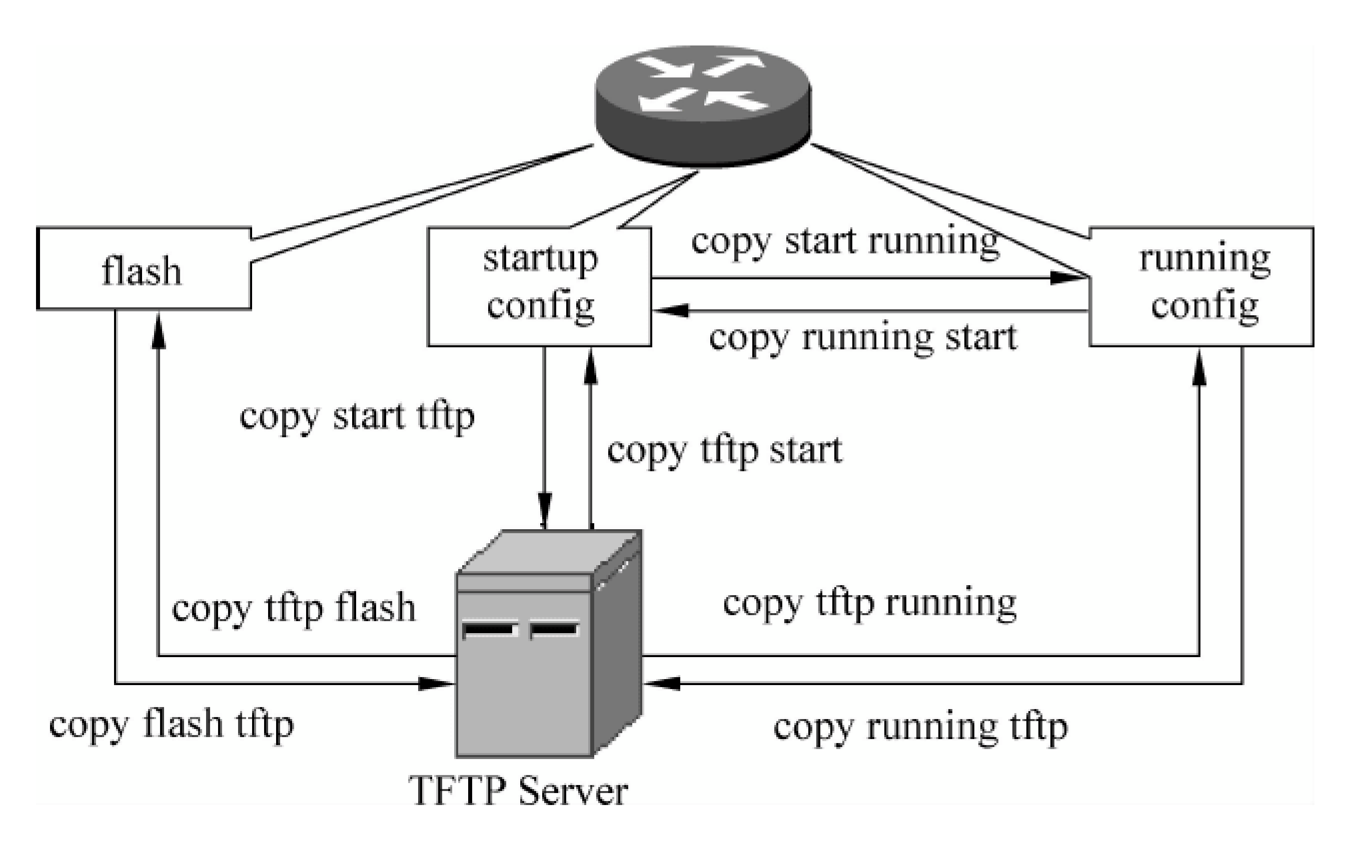


图 5-40　拷贝命令配置格式及应用示意图

(5) 基本设置命令(见表 5-6)

表 5-6 基本设置命令表

任　务	命　令
全局设置	config terminal
设置访问用户及密码	username *username* password *password*
设置特权密码	enable secret *password*
设置路由器名	hostname *name*
设置静态路由	ip route *destination subnet-mask next-hop*
启动 IP 路由	ip routing
启动 IPX 路由	ipx routing
端口设置	interface *type slot/number*
设置 IP 地址	ip address *address subnet-mask*
设置 IPX 网络	ipx network *network*
激活端口	no shutdown
物理线路设置	line *type number*
启动登录进程	login [local|tacacs server]
设置登录密码	password *password*

4. 静态路由的配置

1) 静态路由简介

静态路由是管理员根据网络的情况手动在路由器中配置路由,它不会随着网络拓扑结构的变化而动态地修改,静态路由一经设定就存在于路由表中,在网络结构发生变化后,管理员必须手工修改路由表。

由于静态路由不能对网络的改变做出反应,因此两个运行静态路由的路由器之间是无需进行路由信息交换的,这样就可以节省网络的带宽、提高路由器 CPU 和内存的利用率。静态路由一般用于网络规模不大、拓扑结构固定的网络中。

静态路由的优点是简单、高效、可靠,但是它的网络扩展性较差,配置繁琐,如果要在网络上增加一个新的网段,管理者必须在所有路由器上增加相应的路由,这里因为静态路由不能随网络拓扑的变化而自动发生变化,因此也就限制了静态路由的使用范围。静态路由和动态路由有各自的特点和适用范围,因此静态路由通常作为动态路由的补充在大规模的复

杂网络中使用。当一个数据包在路由器中进行寻址时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发数据，否则再查找动态路由。

2）静态路由的配置

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径。在网络结构比较简单且到达某一网络所经过的路径唯一的情况下采用静态路由。静态路由的命令格式如下：

```
ip route network[mask ]{address|interface}[distance][tag tag][permanent]
```

静态路由中各参数的解释如表 5-7 所示。

表 5-7 静态路由中相关参数的解释

命 令	含 义
network	所要到达的目标网络
mask	目标网络的子网掩码
address	下一跳的 IP 地址，即相邻路由器的端口 IP 地址
interface	本地网络接口，通过这个接口可到达目标网络
distance	管理距离（可选），默认为 1
tag tag	tag 值（可选），在策略路由中，作为路由标记
permanent	指定路由条目在路由表中永远存在

例 5-1 在如图 5-41 所示的网络中，若要实现两个网络的通信，请给出其静态路由的配置方法。

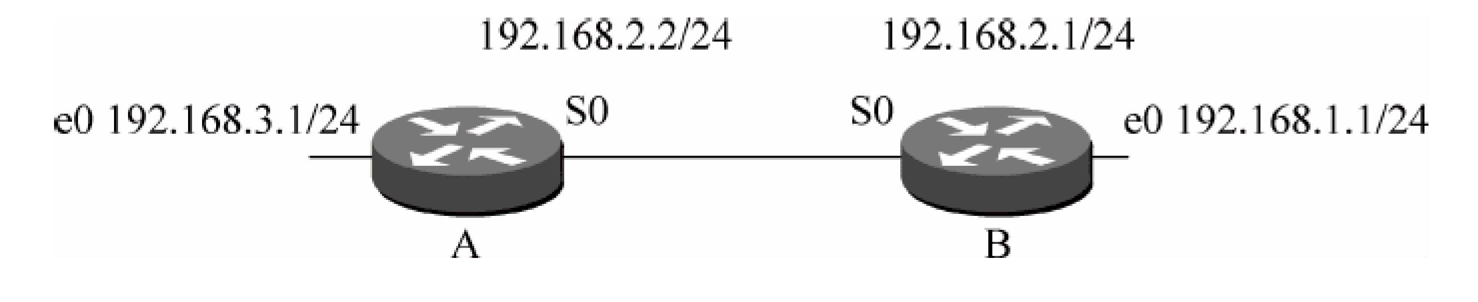


图 5-41 网络连接示例

```
!路由器 A 的静态配置
RouterA(config)#interface ethernet0
RouterA(config-if)#ip address 192.168.3.1 255.255.255.0
RouterA(config)#interface serial0
RouterA(config-if)#ip address 192.168.2.2 255.255.255.0
RouterA(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
!路由器 B 的静态配置
RouterB(config)#interface ethernet0
RouterB(config-if)#ip address 192.168.1.1 255.255.255.0
RouterB(config)#interface serial0
RouterB(config-if)#ip address 192.168.2.1 255.255.255.0
RouterB(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

3）默认路由的配置

默认路由是一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择。如果没有默认路由器，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由在某些时候非常有效，当存在末梢网络时，默认路由会大大简

化路由器的配置,减轻管理员的工作负担,提高网络性能。配置默认路由的命令格式如下:

```
ip route network[mask ]{address|interface}[distance][tag tag][permanent]
```

例 5-2 在例 5-1 中,因为从路由器 A 到路由器 B 只有一条路径,所以可以配置默认路由,方法为:

```
RouterA(config)#interface ethernet0
RouterA(config-if)#ip address 192.168.3.1 255.255.255.0
RouterA(config)#interface serial0
RouterA(config-if)#ip address 192.168.2.2 255.255.255.0
RouterA(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

路由器 B 的配置请读者自己完成。

5. 动态路由

1) 动态路由简介

动态路由是网络中的路由器之间相互通信、传递路由信息、利用收到的路由信息更新路由表的过程。动态路由协议随网络拓扑的变化而动态地修改它的路由表,通过动态路由协议的相应修改,路由器可以保持路由信息的一致性,因此动态路由能够实时地适应网络结构的变化。如果路由更新信息表明网络拓扑发生了变化,路由协议就会重新计算路由表以动态地反映网络拓扑的变化。

动态路由适用于网络规模较大、网络拓扑复杂的网络。当然,各个动态路由协议会不同程度地占用网络带宽和 CPU 资源。

2) OSPF 协议

开放最短路径协议(Open Shortest Path First,OSPF)是一个内部网关协议(Interior Gateway Protocol,IGP),用于在单一自治系统(Autonomous System,AS)内决策路由。与 RIP 相对,OSPF 是链路状态路由协议,而 RIP 是距离向量路由协议。

链路是路由器接口的另一种说法,因此 OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库,生成最短路径树,每个 OSPF 路由器使用这些最短路径构造路由表。

(1) 有关命令

OSPF 配置命令如表 5-8 所示。其中,OSPF 路由进程 *process-id* 必须指定范围在 1~65 535,多个 OSPF 进程可以在同一个路由器上配置,但最好不这样做。多个 OSPF 进程需要多个 OSPF 数据库的副本,必须运行多个最短路径算法的副本。*process-id* 只在路由器内部起作用,不同路由器的 *process-id* 可以不同。*wildcard-mask* 是子网掩码的反码,网络区域 ID *area-id* 在 0-4 294 967 295 内的十进制数,也可以是带有 IP 地址格式的 x. x. x. x。当网络区域 ID 为 0 或 0.0.0.0 时为主干域。不同网络区域的路由器通过主干域学习路由信息。

表 5-8 OSPF 配置命令

任　　务	命　　令
指定使用 OSPF 协议	router ospf *process-id1*
指定与该路由器相连的网络	network *address wildcard-mask* area *area-id2*
指定与该路由器相邻的节点地址	neighbor *ip-address*

(2) 基本配置示例

例 5-3 如图 5-42 所示，网络中的各种参数已经给出，试给出路由器 OSPF 协议的配置过程。

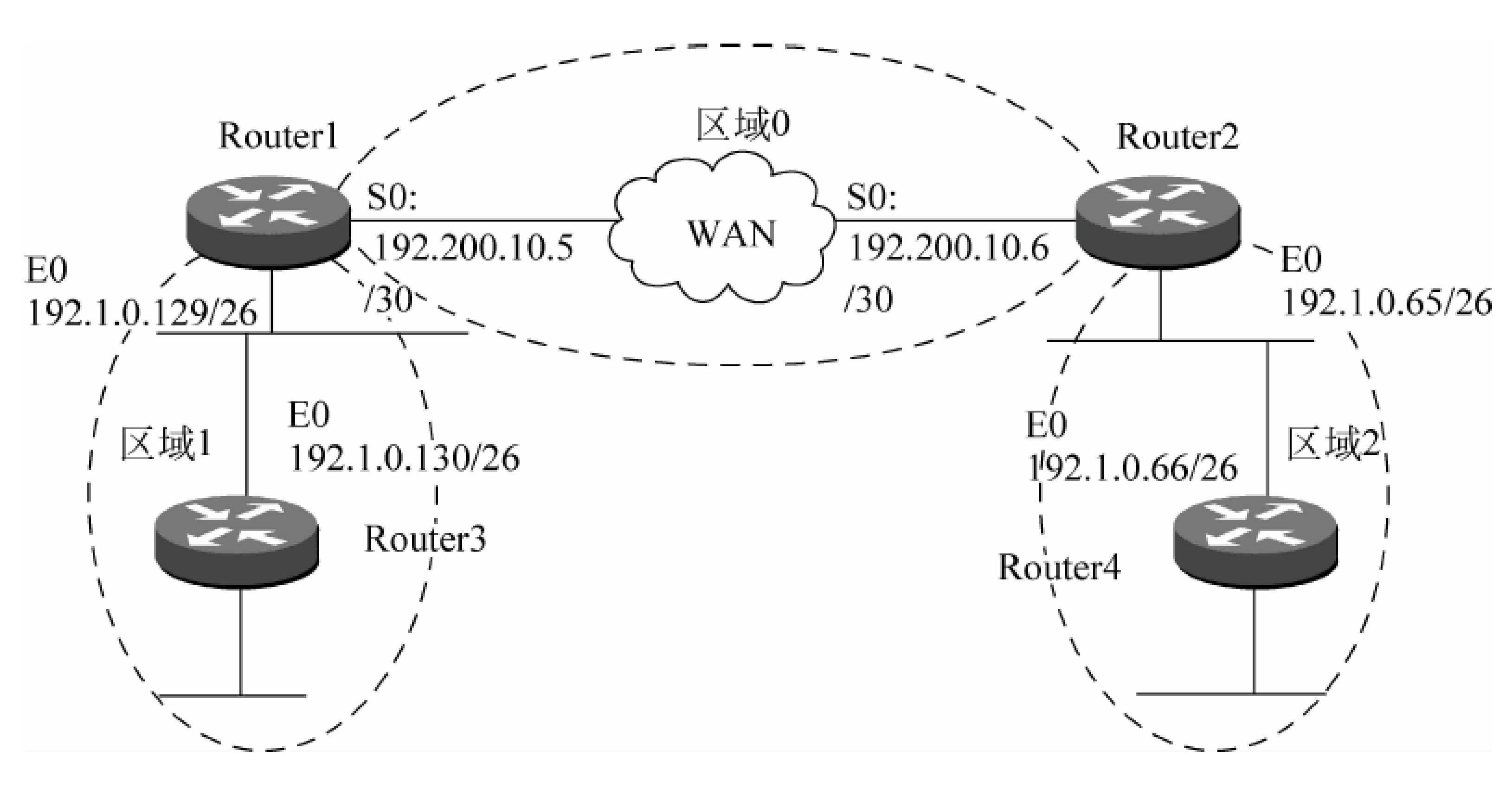


图 5-42 OSPF 配置示意图

```
!Router1 的配置
interface ethernet 0
ip address 192.1.0.129 255.255.255.192
interface serial 0
ip address 192.200.10.5 255.255.255.252
router ospf 100
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1
!Router2 的配置
interface ethernet 0
ip address 192.1.0.65 255.255.255.192
interface serial 0
ip address 192.200.10.6 255.255.255.252
router ospf 200
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.64 0.0.0.63 area 2
!Router3 的配置
interface ethernet 0
ip address 192.1.0.130 255.255.255.192
router ospf 300
network 192.1.0.128 0.0.0.63 area 1
!Router4 的配置
interface ethernet 0
ip address 192.1.0.66 255.255.255.192
router ospf 400
network 192.1.0.64 0.0.0.63 area 1
```

(3) 使用身份验证

出于安全考虑，可以在相同 OSPF 区域的路由器上启用身份验证的功能，只有经过身份验证的同一区域的路由器才能互相通告路由信息。

在默认情况下 OSPF 不使用区域验证。通过纯文本身份验证和消息摘要(md5)身份验证两种方法可启用身份验证功能。纯文本身份验证传送的身份验证口令为纯文本，它会被

网络探测器确定，所以不安全，不建议使用。而消息摘要(md5)身份验证在传输身份验证口令前，要对口令进行加密，所以一般建议使用此种方法进行身份验证。

使用身份验证时，区域内所有的路由器接口必须使用相同的身份验证方法。为启用身份验证，必须在路由器接口配置模式下为区域内的每个路由器接口配置口令，身份验证的命令如表 5-9 所示。

表 5-9　身份验证配置命令

任　　务	命　　令
指定身份验证	area *area-id* authentication [message-digest]
使用纯文本身份验证	ip ospf authentication-key *password*
使用消息摘要(md5)身份验证	ip ospf message-digest-key *keyid* md5 *key*

3) RIP 协议

路由信息协议(Routing information Protocol，RIP)是应用较早、使用较普遍的内部网关协议(IGP)，适用于小型同类网络，是典型的距离向量(distance-vector)协议。

RIP 通过广播 UDP 报文来交换路由信息，每 30s 发送一次路由信息更新。RIP 提供跳跃计数(hop count)作为尺度来衡量路由距离，跳跃计数是一个包到达目标所必须经过的路由器的数目。如果到相同目标有两个不等速或不同带宽的路由器，但跳跃计数相同，则 RIP 认为两个路由是等距离的。RIP 最多支持的跳数为 15，即在源和目的网间所要经过的最多路由器的数目为 15，跳数 16 表示不可达。

(1) 有关命令

RIP 协议的配置命令如表 5-10 所示。

表 5-10　RIP 协议配置命令

任　　务	命　　令
指定使用 RIP 协议	router rip
指定 RIP 版本	version {1|2}
指定与该路由器相连的网络	network *network*

(2) RIP 协议配置示例

例 5-4　如图 5-43 所示，试给出路由器 RIP 协议配置的关键语句。

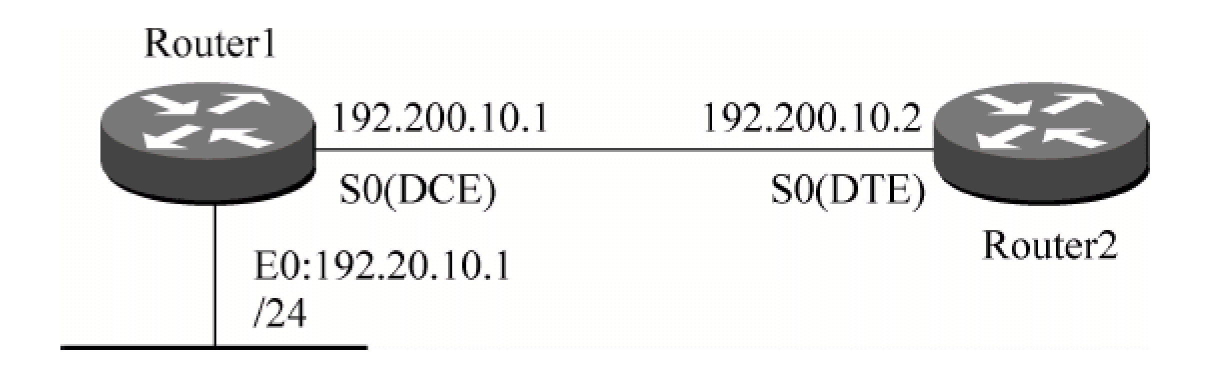


图 5-43　RIP 配置示意图

```
!Router1 的配置的关键语句
router rip
version 2
network 192.200.10.0
network 192.20.10.0
```

其余详细配置由读者自己完成。

5.3.2 ACL 管理

1. 访问控制列表(ACL)

1) 什么是 ACL

ACL 实际上就是一系列允许和拒绝匹配准则的集合,简单地说就是利用这些准则来告诉路由器哪些数据包可以接收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝,要根据这些准则中所定义的条件来决定。匹配准则的种类繁多,可以是数据包目标地址的单项目匹配,也可以是数据包目标地址、源地址、端口等多个项目的综合匹配,访问控制列表对符合匹配规则的数据包进行允许和拒绝的操作。

2) ACL 的类型

(1)标准访问控制列表:标准访问控制列表只使用 IP 数据包的源 IP 地址作为条件测试。通常允许或拒绝的是整个协议簇,不区分 IP 流量类型,如 WWW、Telnet、UDP 等服务。

(2) 扩展访问控制列表:扩展访问控制列表可测试 IP 包的第 3 层和第 4 层报头中的其他字段;可测试源 IP 地址和目的 IP 地址、网络层的报头中的协议字段,以及位于传输层报头中的端口号。

(3) 命名访问控制列表:从技术上来说,ACL 实际上只有两种,命名访问控制列表可以是标准的或扩展的访问控制列表,并不是一种真正的新类型列表。它们的创建和使用同标准的和扩展的访问控制列表不相同,但功能上是一样的。

3) ACL 的配置规则

- 访问控制列表的编号指明了使用何种访问控制列表。
- 每个端口、每个方向、每条协议只能对应一条访问控制列表。
- 访问控制列表的内容决定的数据的控制顺序。
- 具有严格限制的语句放在访问控制列表中所有语句的最上面。
- 在访问控制列表的最后有一条隐含声明:deny any。因此每一条正确的访问控制列表都至少应该有一条允许语句。
- 先创建访问控制列表,然后应用到端口上。
- 访问控制列表不能过滤路由器自己产生的数据。

2. 标准访问控制列表

若想要阻止(允许)来自某一网段的所有通信流量,或要拒绝某一协议簇的所有通信流量时,可以使用标准 ACL 实现这一目标。标准 ACL 通过检查被路由数据包的源地址,从而拒绝或允许基于网络、子网或主机 IP 地址的某一协议簇通过路由器出口。

标准 ACL 语法如下:

```
Router(config)#access-list access-list-number {permit|deny}source [source-wildcard][log]
no ip access-list access-list-number !删除 ACL
Router(config-if)#ip access-group access-list-number {in|out}!在端口上应用 ACL,指明进或出方向,
                                                    默认为出方向
no ip access-group access-list-number !在端口上删除 ACL
```

access-list 命令中参数的用法与含义如表 5-11 所示。

表 5-11　access-list 命令中参数的用法与含义

参　　数	参 数 说 明
access-list-number	访问控制列表号,用来指出入口属于哪一个访问控制列表(其中标准 ACL 为 1～99 间的一个数)
deny| permit	如果满足测试条件,则拒绝|接受从该入口来的通信流量
source	数据包的源地址,可以是主机 IP 地址,也可以是网络地址
source-wildcard	(可选)通配符掩码,用来跟源地址一起决定哪些位需要匹配操作,默认为 0.0.0.0
log	(可选)生成相应的日志信息,用来记录经过的 ACL 入口的数据包的有关情况

例 5-5　在如图 5-44 所示的网络中,要求三个部门间可以进行通信;销售部不能对财务部进行访问,但经理部可以对财务部进行访问。

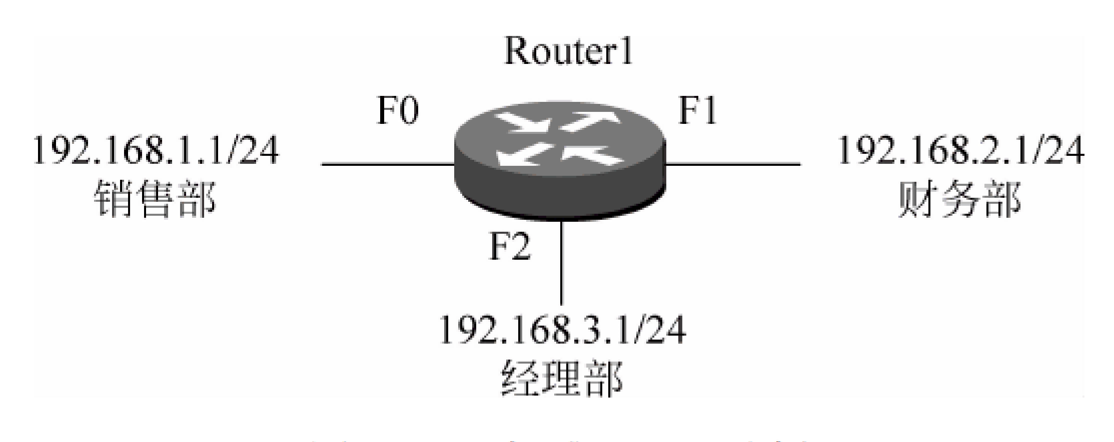


图 5-44　标准 ACL 示例

标准 ACL 参考配置为:

```
!配置标准 ACL
Router1(config)#access-list 1 deny 192.168.1.0 0.0.0.255 !拒绝来自 192.168.1.0 网段的流量通过
Router1(config)#access-list 1 permit 192.168.3.0 0.0.0.255
!将 ACL 应用在相应的接口
Router1(config)#interface fastEthernet 1
Router1(config-if)#ip access-group 1 out
```

例 5-6　在实际应用中控制远程用户登录到一个大型路由器是非常困难的,因为路由器上的活动端口是允许访问的。通过标准 ACL 可以控制 vty(Virtual Terminal)的访问,方法是:

- 创建标准 ACL,只允许希望访问的主机登录。
- 使用 access-class 命令将此 ACL 应用到 vty 线路。

参考配置如下:

```
Router2(config)# access-list 2 permit 192.89.55.0 0.0.0.255
Router2(config)# line vty 0 4
Router2(config-line)# access-class 2 in
```

3. 扩展访问控制列表

如果想实现更加精确的流量控制,可以使用扩展 ACL。扩展 ACL 的测试条件既可以检查数据包的源地址,也可以检查数据包的目的地址。此外,在每个扩展 ACL 条件判断语句的后面部分,还通过一个特定的参数来指定一个可选的 TCP 或 UDP 的端口号。

扩展 ACL 的语法如下(有关参数如表 5-12 所示):

Router(config)# access-list *access-list-number* {permit | deny} protocol source *source-wildcard* destination *detination-wildcard* [operator operand] [established]

表 5-12 扩展 ACL 参数说明

参　数	参数说明
access-list-number	访问控制列表号，用 100～199 间的一个数标识一个 ACL
deny| permit	如果满足测试条件，则拒绝|接受从该入口来的通信流量
protocol	协议类型
source 和 destination	源和目的，标识源和目的地址
source-wildcard 和 destination-wildcard	通配符掩码
operator operand	lt、gt、eq、neq(小于、大于、等于、不等于)一个端口号
established	如果数据包使用一个已建连接，便可允许 TCP 信息量通过

例 5-7 如图 5-45 所示，如果学生所在网段的主机不能使用 FTP 服务器，参考扩展 ACL 配置如下：

```
!配置扩展 ACL
!禁止规定网段对服务器的 ftp 访问
Router3(config)#access-list 101 deny tcp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255 eq ftp
Router3(config)#access-list 101 permit ip any any !允许其他流量通过
!将 ACL 应用在相应的接口
Router3(config)#interface fastEthernet 0
Router3(config-if)#ip access-group 101 in
```

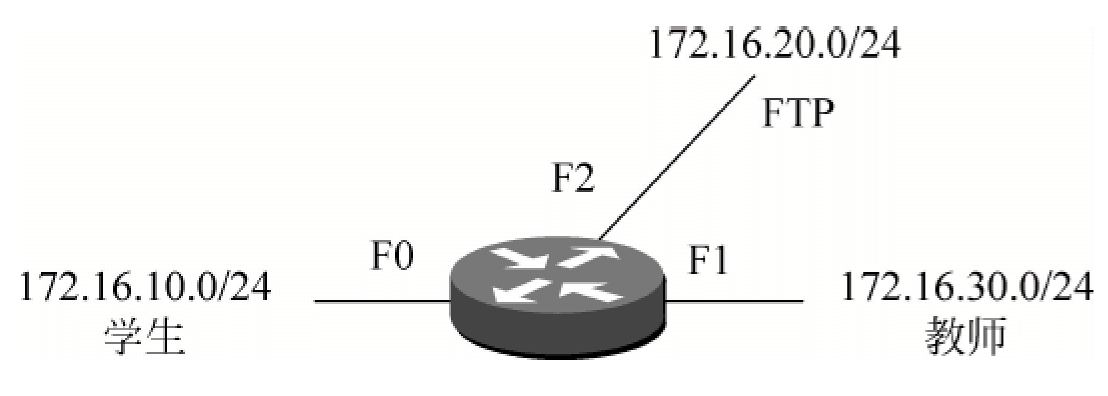


图 5-45 扩展 ACL 示例

4. 命名访问控制列表

命名 ACL 允许在标准 ACL 和扩展 ACL 中，使用一个字母数字组合的字符串(名字)代替前面所使用的数字(1～199)来表示 ACL 表号。命名 ACL 可以用来从 ACL 中删除个别的控制条目，从而方便对 ACL 的修改。

命名 ACL 的语法为：

Router(config)#in access-list {standard|extended} *name*

在 ACL 配置模式下，通过指定一个或多个允许及拒绝条件来决定一个数据包是允许通过还是丢弃，语法格式如下：

Router(config {std-|ext-}nacl)#{permit|deny} {source[source-wildcard]|any}

5.3.3 网络地址转换

1. NAT 概述

1) 为什么需要 NAT

私有 IP 地址只能用于内部寻址，而不能用于访问外部资源，使用网络地址转换(Network Address Translate，NAT)技术可以将多个内部地址映射成少数几个甚至一个合

法的公网 IP 地址，让内部网络中使用私有 IP 地址的设备通过“伪 IP”访问 Internet 等外部资源。NAT 技术不仅很好地解决了 IPv4 地址枯竭的问题，而且给网络带来了一定的安全保障。

2）NAT 的工作原理

如图 5-46 所示，NAT 将网络分为内、外两部分，位于内部网络和外部网络边界的 NAT 路由器执行着地址翻译的操作。

顾名思义，NAT 是一种把内部私有网络地址翻译成合法网络地址的技术。简单地说，NAT 就是在局域网内部使用私有 IP 地址，当需要与外部网络进行通信时，就在网关处将内部地址替换成公用地址。通过使用 NAT 技术，可以只申请一个合法 IP 地址，就把整个局域网中的计算机接入 Internet 中。这时，NAT 屏蔽了内部网络，所有内网资源对于公共网络来说是不可见的，而内部用户通常也不会意识到 NAT 的存在。

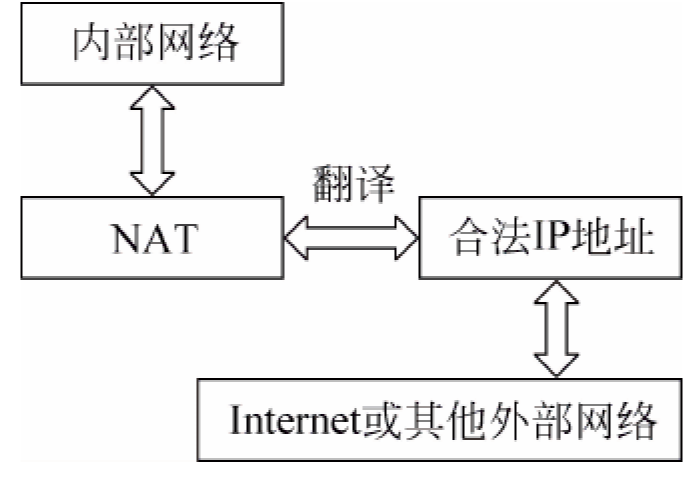


图 5-46 “服务和端口”选项卡

NAT 功能通常被集成到路由器、防火墙、ISDN 路由器或者单独的 NAT 设备中。网络管理员只需在路由器的 IOS 中设置 NAT 功能，就可以实现对内部网络的屏蔽。另外，对小型企业来说，通过软件也可以实现这一功能，例如 5.1.5 节中介绍的 Windows Server 2003 接入服务中也包含了这一功能。

3）NAT 的特点

(1) 将内部网络连接到 Internet。NAT 可以用少数几个甚至一个合法的 IP 地址映射多个内部主机地址，这样就可大大减缓合法 IP 地址耗尽的问题。而且 NAT 修改了数据包的源地址，使外部设备看不到内部设备的地址，因此网络的安全性也得到了一定的保障。

(2) 当变更 ISP 时，虽然 ISP 分配给用户的地址变了，但是用户仍无须改变内部设备的地址，只需在 NAT 路由器上做出相应的修改就可以轻松完成网络的升级，并且 NAT 在网络合并方面也有着很大的应用场合。

(3) 支持 TCP 负载均衡。通过使用 NAT，可以把内部的几台服务器捆绑成一台虚拟服务器，这些服务器在外部设备看来只是一台服务器。当流量进入内部网络时，NAT 可以在这几台服务器之间自动进行分流，这样就增加了网络的可靠性。

4）NAT 功能存在的不足

虽然 NAT 为网络带来了不少好处，但是 NAT 也存在一些不足，主要表现为：

(1) NAT 路由器必须保持对每个连接状态的记录。对于每次翻译的流量，NAT 都必须记住其转换的地址和端口，所以当 NAT 设备出现故障或 NAT 邻近的链路出现故障时，路由难以快速收敛。NAT 也会耗尽大量的 CPU 和内存资源，进而影响网络的性能和数据包的处理，大大增加了网络的延时，这对于部分网络应用程序也是不可接受的。

(2) 在进行一些网络安全的设计和实施时，一些加密方法必须对 IP 包头的完整性进行校验，这样就要求包头在从源到目的地址之间传输时不能被改变。任何在路途中对包头部分的转换都会破坏完整性检查，而 NAT 重写了第三层包头信息，很难实现 IP 包头的完整性。因此在做 IPSec VPN 时，IPSec 不能对 NAT 流量实施端到端的安全保护。

(3) NAT 只能支持有限的程序，NAT 支持的 IP 业务和应用有 HTTP、TFTP、Telnet、NTP、NFS、RCP、RSH、ACHIE、FTP、ICMP、DNS 等。NAT 不支持的 IP 业务和应用有 BOOTP、

SNMP、NETSHOW 等，特别是各种动态路由协议的路由表更新和 DNS 数据库的相互更新。

2. NAT 的类型

NAT 有静态 NAT(Static NAT)、动态 NAT(Pooled NAT)、端口地址转换 PAT(Port Address Translation)三种类型。

(1) 静态 NAT 是指将内部网络的私有 IP 地址转换为公有 IP 地址时，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备的访问。

(2) 动态 NAT 是指将内部网络的私有 IP 地址转换为公有 IP 地址时，IP 地址是不确定的，是随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

(3) 端口地址转换 PAT 是指改变外出数据包的源端口并进行端口转换。在这种方式中，内部网络的所有主机均可共享一个合法外部 IP 地址，实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

3. NAT 的配置

1) 静态 NAT 的配置

静态 NAT 配置的基本步骤如下：

(1) 在端口配置模式下指定接口为内部端口：

```
ip nat inside
```

(2) 在端口配置模式下指定接口为外部端口：

```
ip nat outside
```

(3) 在全局配置模式下，在内部本地地址与内部全局地址之间建立静态地址转换：

```
ip nat inside source static inside-local-address inside-global-address
```

其中参数 *inside-local-address* 指定内部本地地址；*inside-global-address* 指定内部全局地址。

例 5-8 实现静态 NAT 地址转换功能。将 f0/0 作为内部端口，s0/0 作为外部端口，其中 192.168.2.1，172.16.1.1 的内部本地地址采用静态地址转换，其内部合法地址分别对应 194.168.1.1，194.168.1.2。

配置代码如下：

```
RouterA(config)#int f0/0
RouterA(config-if)#ip address 192.168.2.1 255.255.255.0
RouterA(config-if)#ip nat inside
RouterA(config)#int s0/0
RouterA(config-if)#ip address 172.16.1.1 255.255.255.0
RouterA(config-if)#ip nat outside
RouterA(config-if)#clock rate 64000
```

```
RouterA(config)#ip nat inside source static 192.168.2.1 194.168.1.1
RouterA(config)#ip nat inside source static 192.168.2.2 194.168.1.2
RouterA(config)#ip route 0.0.0.0 0.0.0.0 s0/0 !设置默认路由
```

2）动态 NAT 的配置

动态 NAT 配置的基本步骤为：

(1) 在端口配置模式下，指定接口为内部端口：

```
ip nat inside
```

(2) 在端口配置模式下，指定接口为外部端口：

```
ip nat outside
```

(3) 在全局配置模式下，定义内部全局地址池：

ip nat pool *name start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}

各参数的说明见表 5-13。

表 5-13 参数说明表

参　　数	说　　明
name	地址池名字，地址池名在路由器上应该是唯一的
start-ip	定义起始 IP 地址，地址池范围的起始地址
end-ip	定义终止 IP 地址，地址池范围的终止地址
netmask *netmask*	子网掩码，定义地址池中地址的子网掩码
prefix-length *prefix-length*	定义在地址中地址的子网掩码的位数，即前缀长度

(4) 在全局配置模式下，定义一个标准的 access-list 以允许哪些内部本地地址可以进行动态地址转换：

access-list *access-list* permit *source source-wildcard*

其中，*access-list* 表示访问列表号，其标号为 1～99 之间的整数，*source source-wildcard* 为源地址和源地址的通配符。

(5) 在全局配置模式下，在内部的本地地址与内部的全局地址之间复用动态地址转换：

ip nat inside source list {*access-list-number* | *name*} pool *name*

其中，*access-list-number* 表示访问列表号，*name* 表示地址池的名字。

例 5-9 实现动态 NAT 地址转换功能。将 f0/0 作为内部端口，其地址为 192.168.2.1；s0/0 作为外部端口，其地址为 200.168.10.1；其中 200.168.10.2～200.168.10.12 为合法地址池，其内部地址为 192.168.2.0。

实现本例要求的配置代码如下：

```
RouterA(config)#int f0/0
RouterA(config-if)#ip address 192.168.2.1 255.255.255.0
RouterA(config-if)#ip nat inside
RouterA(config)#int s0/0
RouterA(config-if)#ip address 200.168.10.1 255.255.255.0
RouterA(config-if)#ip nat outside
```

```
RouterA(config-if)#clock rate 64000
RouterA(config)#ip nat pool p1 200.168.10.2 200.168.10.12 netmask 255.255.255.0
RouterA(config)#ip nat inside source list 1 pool p1
RouterA(config)#access-list 1 permit 192.168.2.0 0.0.0.255
RouterA(config)#ip route 0.0.0.0 0.0.0.0 s0/0
```

3）PAT 的配置

PAT 配置的基本步骤为：

(1) 在端口配置模式下，指定接口为内部端口：

```
ip nat inside
```

(2) 在端口配置模式下，指定接口为外部端口：

```
ip nat outside
```

(3) 在全局配置模式下，定义内部全局地址池：

ip nat pool name *start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}

(4) 在全局配置模式下，定义一个标准的 access-list 以允许哪些内部本地地址可以进行 PAT：

access-list *access-list* permit *source source-wildcard*

其中，*access-list* 表示访问列表号，其标号为 1～99 之间的整数，*source source-wildcard* 为源地址和源地址的通配符。

(5) 在全局配置模式下，在内部的本地地址与内部的全局地址之间建立 PAT：

ip nat inside source list {*access-list-number* | *name*} pool *name* [overload]

其中，*access-list-number* 表示访问列表号，*name* 表示地址池的名字，overload 指定 NAT 翻译类型，多个内部本地地址可以使用一个内部全局地址，即 PAT。

例 5-10 实现动态 NAT 地址转换功能。某企业从 ISP 获得的合法地址范围为 192.1.1.100～192.1.1.200，企业内部有销售(sell)、财务(count)、经理部(manager)和临时公用部门(temp)。其中，临时公用部门使用 overload 技术。

实现本例的配置代码如下：

```
interface Ethernet0
ip address 172.18.150.150 255.255.0.0
ip nat inside
interface Serial0
ip address 192.1.1.161 255.255.255.252
ip nat outside
! 定义从 ISP 那里申请到的 IP 在企业内部的分配策略。
ip nat pool sell 192.1.1.100 192.1.1.120 netmask 255.255.255.0
ip nat pool count 192.1.1.121 192.1.1.150 netmask 255.255.255.0
ip nat pool manager 192.1.1.180 192.1.1.200 netmask 255.255.255.0
ip nat pool temp 192.1.1.155 192.1.1.160 netmask 255.255.255.0
!将访问列表与地址池对应，以下为动态地址转换。
ip nat inside source list 1 pool sell
```

```
ip nat inside source list 2 pool count
ip nat inside source list 3 pool manager
!将访问列表与地址池对应,以下为复用动态地址转换。
ip nat inside source list 4 pool temp overload
!将访问列表与地址池对应,以下为静态地址转换
ip nat inside source static 172.18.100.168 192.1.1.168
ip nat inside source static 172.18.100.169 192.1.1.169
ip route 0.0.0.0 0.0.0.0 Serial0
!内部网访问地址表,他指出内部网络能访问外部网的地址段,分别定义是为了对应不同的地址池。
access-list 1 permit 172.18.101.0 0.0.0.255
access-list 2 permit 172.18.105.0 0.0.0.255
access-list 3 permit 172.18.108.0 0.0.0.255
access-list 4 permit 172.18.112.0 0.0.0.255
```

4）基于 NAT 的 TCP 负载均衡的配置

(1) 基于 NAT 的 TCP 负载均衡技术及应用

NAT 翻译都是从内到外的翻译,即对内部主机发送的数据包的源地址进行翻译。而 NAT 在 TCP 负载均衡上的应用是对外部发往内部的数据包的目标地址进行翻译。

(2) 配置方法

① 在端口配置模式下指定接口为内部端口:

```
ip nat inside
```

② 在端口配置模式下指定接口为外部端口:

```
ip nat outside
```

③ 在全局配置模式下,定义内部全局地址池,地址池中的地址就是用于负载均衡的内部服务器的内部地址:

ip nat pool *name start-ip end-ip* {*netmask netmask* | prefix-length *prefix-length*} <*type rotary*>

参数说明同前,其中 type rotary 可选参数,指示在发生 TCP 负载均衡时,外部主机按照循环的方式来访问虚拟服务器所代表的内部主机。

④ 在全局配置模式下,定义一个标准的 access-list 以允许哪些内部全局地址可以进行地址转换:

access-list *access-list-number* permit *source source-wildcard*

其中,*access-list-number* 是访问列表号,其标号为 1～99 之间的整数;*source source-wildcard* 是源地址和源地址的通配符。

⑤ 在全局配置模式下,在内部的本地地址与内部全局地址之间建立地址转换:

ip nat inside destination list {*access-list-number* | *name*} pool *name*

例 5-11　内部服务器 192.168.1.1、192.168.1.2 和 192.168.1.3 组成一个服务器组,它们共同虚拟成一台虚拟服务器 202.1.23.8,当外部主机对虚拟服务器 202.1.23.8 进行访问时,NAT 路由器将 TCP 会话轮流分配给这个服务器中的成员,NAT 以循环的方式将外部发来的连接的目标地址轮流地翻译成 3 台服务器的实际内部地址,由 3 台服务共同处

理外部主机的通信。

配置步骤如下：

```
RouterA(config)#interface Ethernet0/0
RouterA(config-if)#ip address 192.168.1.8 255.255.255.0
RouterA(config-if)#ip nat inside
RouterA(config)#interface Serial0/1
RouterA(config-if)#ip address 172.16.1.1 255.255.255.0
RouterA(config-if)#ip nat outside
RouterA(config-if)#clock rate 64000
RouterA(config)#ip nat pool V-ser 192.168.1.1 192.168.1.3 prefix-length 24 type rorary
RouterA(config)#ip nat inside destination list pool V-ser
RouterA(config)#access-list 1 permit 202.1.23.8
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1
```

5）基于 NAT 服务分配的配置

(1) 基于 NAT 服务分配技术及应用

在 NAT 的高级应用中，NAT 还可以自动地根据外部过来的流量类型将不同的流量分发给内部的各个应用服务器。例如，在企业网络中，可以将 Web、FTP、E-mail 等服务器组成一台虚拟服务器，外部网络只能看到这台虚拟服务器。当外部用户访问这个虚拟服务器时，NAT 路由器会根据用户的流量类型自动地在企业内部的几台服务器之间自动分流。

(2) 配置方法

① 在端口配置模式下指定接口为内部端口：

```
ip nat inside
```

② 在端口配置模式下指定接口为外部端口：

```
ip nat outside
```

③ 在全局配置模式下定义内部本地服务器和虚拟服务器的地址映射以及端口映射：

ip nat inside source static {tcp|udp} *local-ip-address port-number global-ip address port-number* {*extendable*}

参数说明如表 5-14 所示。

表 5-14 参数说明表

参 数	说 明
tcp|udp	用来指定访问内部服务器所使用的传输层协议(TCP 或 UDP)
local-ip-address port-number	指定内部服务器的内部本地地址和端口号
global-ip address port-number	指定虚拟服务器的内部全局地址和端口号
Extendable	指明有多个内部本地地址可以映射到一个内部全局地址上，此命令为可选，如果不加，系统会自动替用户输入

例 5-12 一企业内部有两台服务器，一台是 Web 服务器，其内部本地地址为 192.168.2.50；另一台是 FTP 服务器，本地地址是 192.168.2.51；这两台服务器共同虚拟在同一台服务器 206.35.35.1。

当外部主机访问 206.35.35.1 时，NAT 路由器除了检查数据包的目标地址，还要检查它的目标端口，如果目标端口是 80，NAT 路由器查询翻译表，然后将数据包的目标翻译成 HTTP 服务器地址 192.168.2.50；如果端口号是 21，NAT 路由器查询翻译表，然后将数据包的目标地址翻译成 FTP 的服务器地址 192.168.2.51。因此，基于 NAT 的服务分配可以非常灵活地部署企业内部服务器，也可以大大节省网络地址的使用。配置步骤为：

```
RouterA(config)#interface Ethernet0/0
RouterA(config-if)#ip address 192.168.215.1 255.255.255.0
RouterA(config-if)#ip nat inside
RouterA(config)#interface Serial0/1
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#ip nat outside
RouterA(config-if)#clock rate 64000
RouterA(config)#ip nat inside source static tcp 192.168.2.51 21
206.35.35.1 20 extendable
RouterA(config)#ip nat inside source static tcp 192.168.2.50 80
206.35.35.1 80 extendable
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1
```

5.3.4 VPN 管理

1. VPN 技术

VPN(Virtual Private Network，虚拟专用网)能够模拟点对点专用链接的方式，通过 Internet 或 Intranet 在两台计算机之间发送数据，是“线路中的线路”，具有良好的保密性和抗干扰性。虚拟专用网提供了一个通过公用网络安全地对企业内部专用网络进行远程访问的连接方式，是对企业内部网的扩展，可以帮助远程用户、企业分支机构、商业伙伴及供应商同企业的内部网建立可信的安全连接，并保证数据的安全传输。在虚拟专用网中的主机将不会觉察到公共网络的存在，仿佛所有的主机都处于一个内部网络中一样。

VPN 大致可以分为远程接入 VPN 和站点与站点 VPN 两大类。其中，远程接入 VPN 又可分为 IPSec 和 SSL VPN 两类。借助远程接入 VPN，用户可以远程廉价、安全地接入企业网络。借助站点与站点 VPN 可以实现分支机构和远程机构与企业总部的远程廉价、安全连接。

利用 IPSec 提供远程接入能够建立最增强型的可定制连接。利用 IPSec 用户几乎可以访问任何应用，就好像自己与总部局域网建立了实际连接一样。IPSec 远程接入具有高度可定制性，利用提供的 API 管理员可以编写执行程序及其他定制程序。

SSL VPN 只使用 Web 浏览器及其本地 SSL 加密，不需要预装 VPN 客户端软件，就能够从可以接入互联网的任何位置远程访问网络资源。利用 Web VPN 能够容易地访问多种企业应用，包括 Web 资源、Web 型应用、Windows Active Directory 文件共享(Web 型)、电子邮件以及基于 TCP 的其他应用，例如来自与互联网相连、可以到达 HTTP 互联网站点的任何计算机的 Telnet 或 Windows 终端服务等。

2. VPN 的配置命令

(1)启用 aaa(验证，授权，审计)认证模式

```
aaa new-model
```

(2) aaa 认证模式和方法设置

```
aaa authentication {login|ppp|enable} {default|列表名称} {enable|krb5|line|local|none|group radius
|group tacacs+}
```

其中，login、ppp 和 enable 为三种认证模式；enable、krb5、line、local、none、group radius、group tacacs+为认证方法。

(3) aaa 授权模式和方法配置

```
aaa authorization {auth-proxy | network |exec | command level |reverse-access |configuration | ip
mobile} {default|list-name} [method1[method2...]
```

(4) 定义 ISAKMP 策略

```
crypto isakmp policy number !最后的数字越小，应用的优先级越高。
```

(5) 定义组

```
crypto isakmp client configuration group 组名
!选择了 Local 授权方式，必须在路由器上使用以上命令定义组。
```

(6) 定义传输数据和完整性验证的策略

```
crypto ipsec transform-set 传输集名 esp-aes esp-sha-hmac
```

(7) 定义 map

```
crypto map 名字 isakmp authorization list 列表名
```

3. VPN 的配置

例 5-13 下面以实例说明 VPN 的配置过程。

(1) 配置 IKE

Internet 密钥交换(IKE)解决了在不安全的网络环境中安全地建立或更新共享密钥的问题。IKE 可用于协商虚拟专用网(VPN)，也可用于远程用户访问安全主机或网络，支持客户端协商。IKE 属于一种混合型协议，由 Internet 安全关联和密钥管理协议(ISAKMP)和两种密钥交换协议 OAKLEY 与 SKEME 组成。

```
router(config)# crypto isakmp enable                  !启用 IKE(默认是启动的)
router(config)# crypto isakmp policy 100              !建立 IKE 策略，优先级为 100
router(config-isakmp)# authentication pre-share       !使用预共享的密码进行身份验证
router(config-isakmp)# encryption des                 !使用 des 加密方式
router(config-isakmp)# group 1                        !指定密钥位数，group 2 安全性更高，但更耗 CPU
router(config-isakmp)# hash md5                       !指定 hash 算法为 MD5(其他方式：sha，rsa)
router(config-isakmp)# lifetime 86400                 !指定 SA 有效期时间，默认 86400 秒，两端要一致
```

(2) 配置密钥 Keys

```
router(config)# crypto isakmp key cisco1234 address 10.0.0.2
!设置要使用的预共享密钥，并指定 VPN 另一端路由器的 IP 地址
```

(3)配置 IPSec

```
router(config)# crypto ipsec transform-set abc esp-des esp-md5-hmac
```

```
!配置 IPSec 交换集 abc
router(config)# crypto ipsec security-association lifetime 86400
!IPSec 安全关联存活期,也可不配置,在下面的 map 里指定即可
router(config)# access-list 110 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
router(config)# access-list 110 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

(4) 配置 IPSec 加密映射

```
router(config)# crypto map mymap 100 ipsec-isakmp          !创建加密图
router(config-crypto-map)# match address 110               !用 ACL 来定义加密的通信
router(config-crypto-map)# set peer 10.0.0.2               !标识对方路由器 IP 地址
router(config-crypto-map)# set transform-set abc           !指定加密图使用的 IPSec 交换集
router(config-crypto-map)# set security-association lifetime 86400
router(config-crypto-map)# set pfs group 1
```

(5) 应用加密图到接口

```
router(config)# interface ethernet0/1
router(config-if)# crypto map mymap
```

5.4 网络隔离设备管理

面对新型网络攻击手段的出现和高安全度网络对安全的特殊需求,全新安全防护防范理念的网络安全技术——“网络隔离技术”应运而生。网络隔离技术的目标是确保隔离有害的攻击,在可信网络之外和保证可信网络内部信息不外泄的前提下,完成网间数据的安全交换。

5.4.1 网络隔离

1. 网络隔离的概念

网络隔离主要是指把两个或两个以上可路由的网络通过不可路由的协议(如 IPX/SPX、NetBEUI 等)进行数据交换而达到隔离的目的。由于其原理主要是采用了不同的协议,所以通常也叫协议隔离。1997 年,信息安全专家 Mark Joseph Edwards 在他编写的《Understanding Network Security》一书中,就对协议隔离进行了归类。在书中他明确地指出了协议隔离和防火墙不属于同类产品。

2. 网络隔离技术的发展

隔离概念是在为了保护高安全度网络环境的情况下产生的。隔离产品的大量出现,也是经历了五代隔离技术不断的实践和理论相结合后得来的。

第一代隔离技术——完全的隔离。此方法使得网络处于信息孤岛状态,做到了完全的物理隔离,需要至少两套网络和系统,更重要的是信息交流的不便和成本的提高,给维护和使用带来了极大的不便。

第二代隔离技术——硬件卡隔离。在客户端增加一块硬件卡,客户端硬盘或其他存储设备首先连接到该卡,然后再转接到主板上,通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时,同时选择了该卡上不同的网络接口,连接到不同的网络。但是,这种隔离产品有的仍然需要网络布线为双网线结构,产品存在着较大的安全隐患。

第三代隔离技术——数据转播隔离。利用转播系统分时复制文件的途径来实现隔离，切换时间非常之长，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

第四代隔离技术——空气开关隔离。它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在有许多问题。

第五代隔离技术——安全通道隔离。此技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

3. 网络隔离的原理

第五代隔离技术的实现原理是通过专用通信设备、专有安全协议和加密验证机制及应用层数据提取和鉴别认证技术，进行不同安全级别网络之间的数据交换，彻底阻断了网络间的直接 TCP/IP 连接，同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了网间数据交换的安全、可控，杜绝了由于操作系统和网络协议自身漏洞带来的安全风险。

5.4.2 网络隔离设备

1. 物理隔离

所谓“物理隔离”是指内部网不直接或间接地连接公共网。物理隔离的目的是保护路由器、工作站、网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击。只有使内部网和公共网物理隔离，才能真正保证内部网络不受来自互联网的黑客攻击。此外，物理隔离也为内部网划定了明确的安全边界，使得网络的可控性增强，便于内部管理。物理隔离常见的方式有物理安全隔离卡、物理隔离集线器、物理隔离网闸等。

(1) 物理安全隔离卡

物理安全隔离卡是物理隔离的低级实现形式，一个物理安全隔离卡只能管一台个人计算机，甚至只能在 Windows 环境下工作，每次切换都需要开关机一次。物理安全隔离卡的功能即是以物理方式将一台 PC 虚拟为两个计算机，实现工作站的双重状态，既可在安全状态，又可在公共状态，两个状态是完全隔离的，从而使一台工作站可在完全安全状态下联接内、外网。物理安全隔离卡实际是被设置在 PC 中最低的物理层上，通过卡上一边的 IDE 总线连接主板，另一边连接 IDE 硬盘，内、外网的连接均须通过网络安全隔离卡。PC 硬盘被物理分隔成为两个区域，在 IDE 总线物理层上，在固件中控制磁盘通道，在任何时候，数据只能通往一个分区。

在安全状态时，主机只能使用硬盘的安全区与内部网连接，而此时外部网连接是断开的，且硬盘的公共区的通道是封闭的。在公共状态时，主机只能使用硬盘的公共区，可以与外部网连接，而此时与内部网是断开的，且硬盘安全区也是被封闭的。

(2) 物理隔离集线器

物理隔离集线器也称作网络安全隔离(hub)，是一种多路开关切换设备，它与物理安全隔离卡配合使用。它具有标准的 RJ-45 接口，入口与物理安全隔离卡相连，出口分别与内、外网络的 hub 相连。它检测物理安全隔离卡发出的特殊信号，识别出所连接的计算机，自

动将其网络线切换至相应的网络 hub 上。实现多台独立的安全计算机与内外两个网络的安全连接以及自动切换,进一步提高了系统的安全性,并且解决了多网布线问题,可以让连接两个网络的安全计算机只通过一条网络线即可与多网切换连接。对现存网络改进有较大帮助。

(3) 物理隔离网闸

物理隔离网闸,是利用双主机形式,从物理上来隔离阻断潜在攻击的连接。其中包括一系列的阻断特征,如没有通信连接,没有命令,没有协议,没有 TCP/IP 连接,没有应用连接,没有包转发,只有文件"摆渡",对固态介质只有读和写两个命令。其结果是无法攻击,无法入侵,无法破坏。

物理隔离网闸的硬件主要包括三部分,分别是专用安全隔离切换装置(数据暂存区)、内部处理单元和外部处理单元。系统中的专用安全隔离切换装置分别连接内部处理单元和外部处理单元。这种独特和巧妙的设计,保证了安全隔离切换装置中的数据暂存区在任一时刻仅连通内部处理单元或者外部处理单元,从而实现内外网的安全隔离。

2. 逻辑隔离器

逻辑隔离器也是一种不同网络间的隔离部件,被隔离的两端仍然存在物理上数据通道连线,但通过技术手段保证被隔离的两端没有数据通道,即逻辑上隔离。一般使用协议转换、数据格式剥离和数据流控制的方法,在两个逻辑隔离区域中传输数据,并且传输的方向是可控状态下的单向。不能在两个网络之间直接进行数据交换。

5.4.3 网络隔离方案

1. 单内网解决方案

如图 5-47 所示,这种方案适合小型的单网结构的局域网。在一些小规模的部门中,由于功能比较单一,没有必要划分几个网络,同时为节约成本,只有部分工作站节点需要单独通过 Modem 等拨号设备接入 Internet。这样可以在需要接入 Internet 的工作站节点计算机上安装物理隔离产品,让其能够在与网络隔离的状态下拨号上网,确保网络的安全。

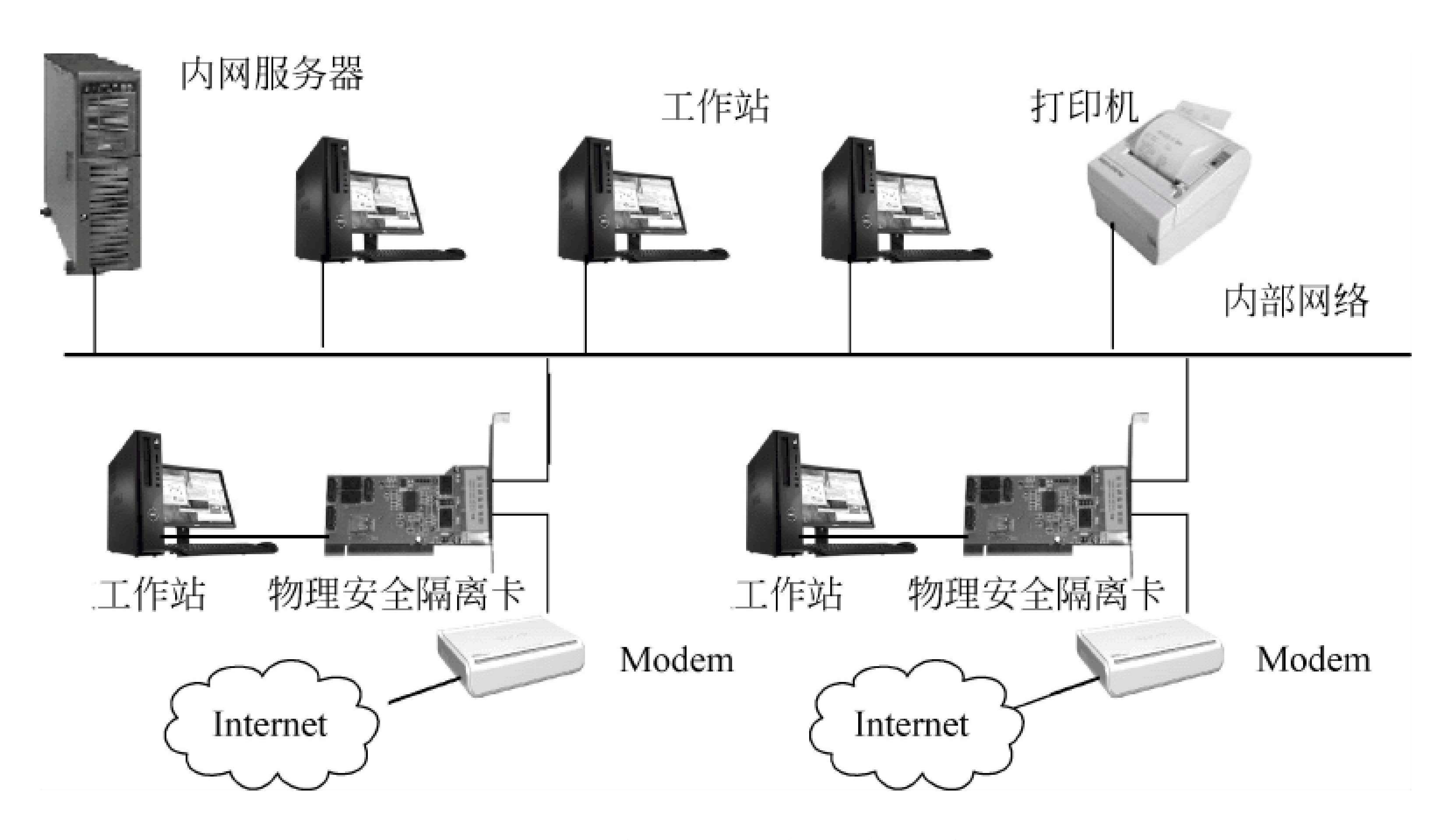


图 5-47 单内网解决方案示意图

2. 双布线双网解决方案

如图 5-48 所示，这种方案适合中大型机构的局域网布局，在这里，某个机构内的网络分为内部涉密网和公共网，其中公共网通过集中出口连接 Internet（视需要也要安装防火墙、入侵检测及防病毒等措施），部分计算机需要能够接入两个网络，但同时又要保证内外网的完全物理隔离。还有一些机构的网络由于内部功能的划分，本身就有几个分离的网络，采用物理隔离方法将更好地把这些网络整合在一起，变为一个全范围公共网加上几个内部安全子网的多网互动的有效网络格局。

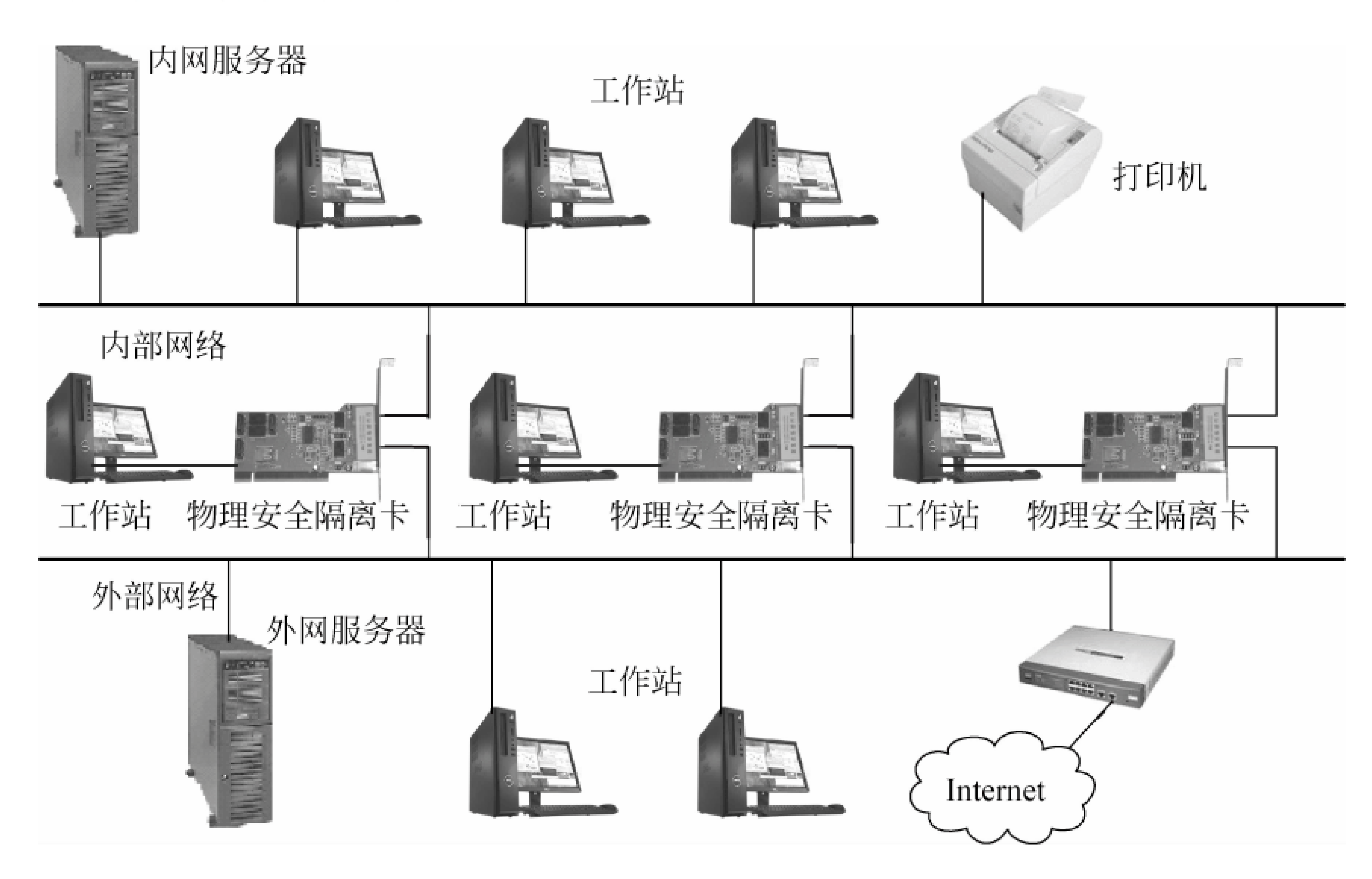


图 5-48　双布线双网解决方案示意图

3. 单布线连接双网方案

如图 5-49 所示，物理隔离集线器与安装了物理安全隔离卡的安全计算机配合使用可以满足对单网布线的要求，即桌面计算机只用一条网线就可连接到远端的双网上。如果用户因某种原因无法使用双网布线时，可采用此方案。

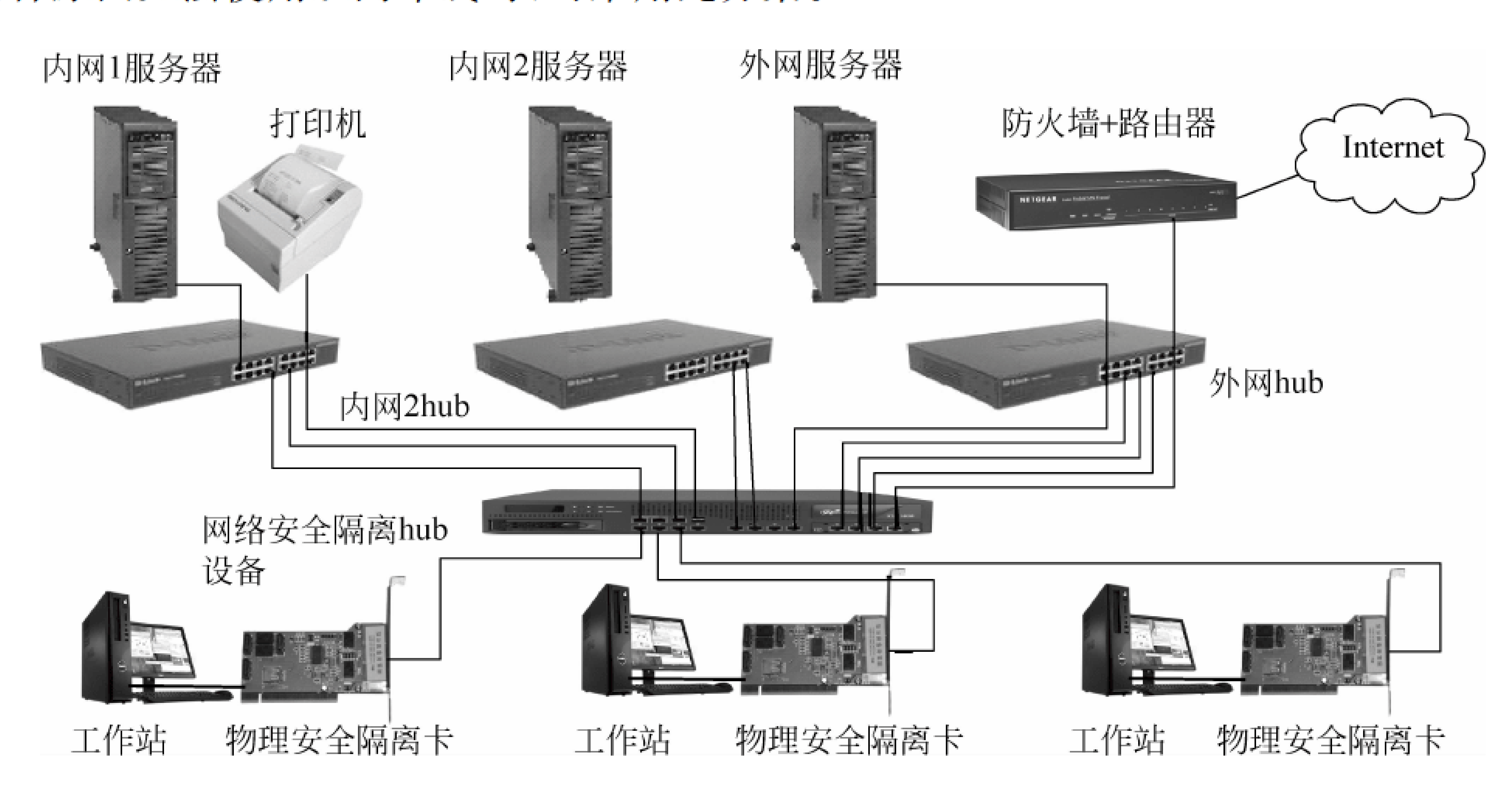


图 5-49　单布线连接双网示意图

5.5 电源管理

目前，UPS已经成了企业网络中不可或缺的重要组成部分。当市电不稳或停电时，UPS可以提供安全的供电保证，保障网络设备的正常运行。UPS虽然可以在市电发生异常时使网络设备免于遭受突然断电的危险，但并不意味着可以就此高枕无忧了。UPS备用的时间是有限的，当UPS电池储存的电能耗尽时，同样会导致网络的瘫痪，所以掌握UPS的供电情况，需要对UPS进行管理和监视。

5.5.1 UPS智能化管理工具

1. Winpower简介

Winpower是山特UPS监控软件，它既支持单台独立的计算机，也支持在网络内的所有计算机。

Winpower用于监控UPS，保证计算机系统不会因为市电的故障而遭到损坏。通过Winpower软件，用户可以在一台计算机上监控局域网内任意一台UPS；通过Winpower软件，一台UPS同时可以对网络上多台计算机提供安全保护，包括在市电故障时安全关闭系统、保存应用程序数据、关闭UPS等。

2. Winpower的结构组成

Winpower包括Agent（代理）、Monitor（监视器）和任务栏图标三部分。

（1）Agent是Winpower的核心，作为系统的一个服务程序运行在后台。Agent负责与UPS进行通信，记录UPS事件，通知用户异常事件的发生，根据用户要求采取某些措施，需要时可关闭计算机系统及UPS。同时，Agent可以由Monitor来设定管理。

（2）Monitor是Winpower的用户界面程序。运行时与Agent通信。通过Monitor，用户可以查看本地UPS实时状态信息、服务器信息，并且允许用户修改UPS的工作参数。Monitor可以运行在局域网中的任意一台计算机或单独的一台计算机之上。

（3）任务栏图标是Winpower的管理工具，运行时在系统任务栏的状态区中显示Winpower的图标。当启动Winpower软件或计算机启动并登录后，在桌面右下角将会自动启动一个绿色电源图标。

3. 山特UPS监控解决方案

（1）Winpower标准版监控软件

该方案可以通过串口通信方式，对近距离单台UPS进行监控，实时了解UPS的市电、负载、电池等状态信息。当UPS运行的环境出现异常时，通过系统广播、电子邮件、手机短信等方式及时通知管理人员。当电池将耗尽时，可以设置安全关闭计算机系统。如图5-50所示为小型企业办公室UPS监控应用拓扑图。

（2）Winpower企业版集中监控解决方案

该方案可以通过串口和网络两种方式对多台UPS进行集中监控，在一个界面上实时了解各UPS的状况，远程操作与维护UPS。当任意一个UPS的运行环境出现异常时，可以通过各种方式第一时间通知到相关人员。如图5-51所示为集团与分部UPS监控应用拓扑图。

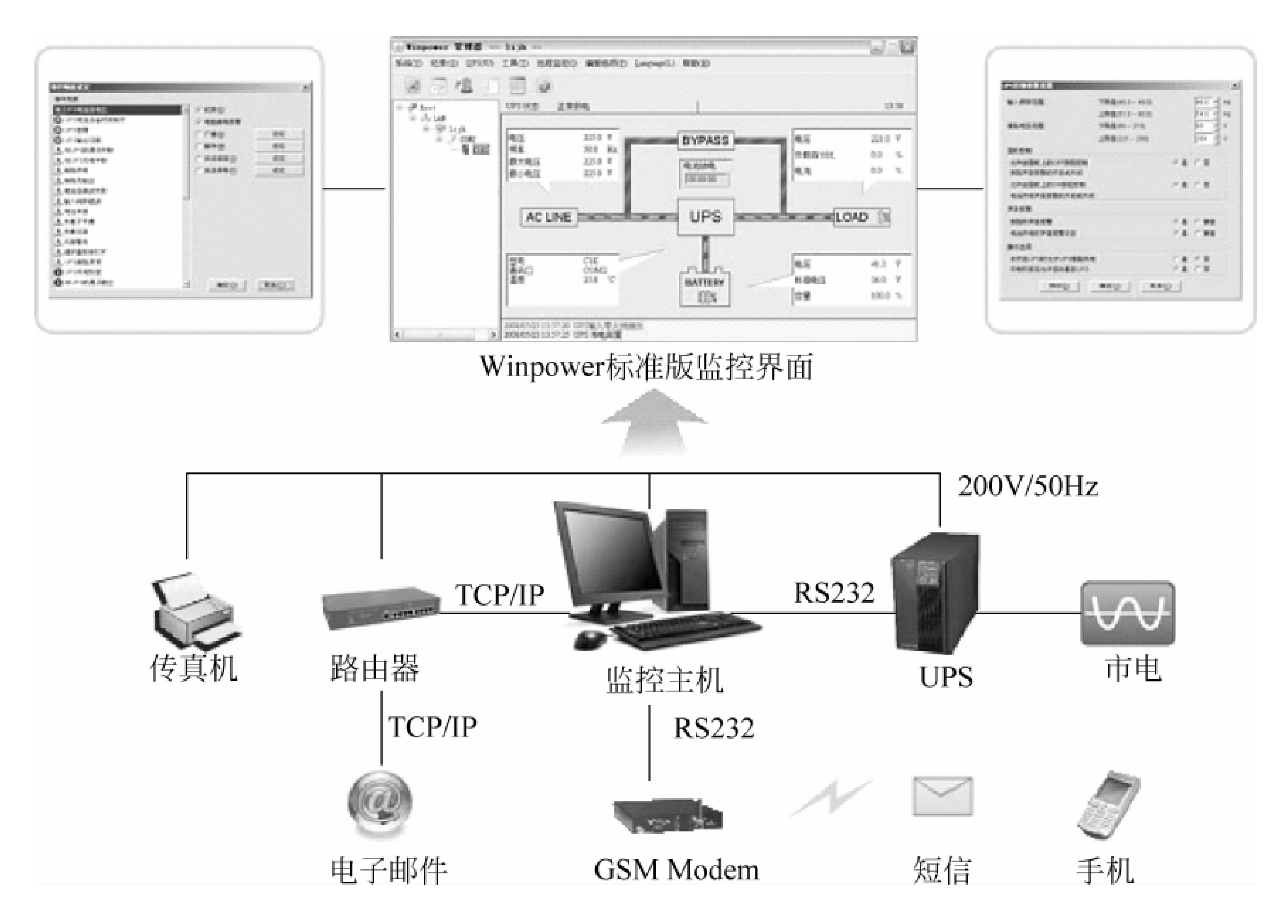


图 5-50　小型企业办公室 UPS 监控应用拓扑图

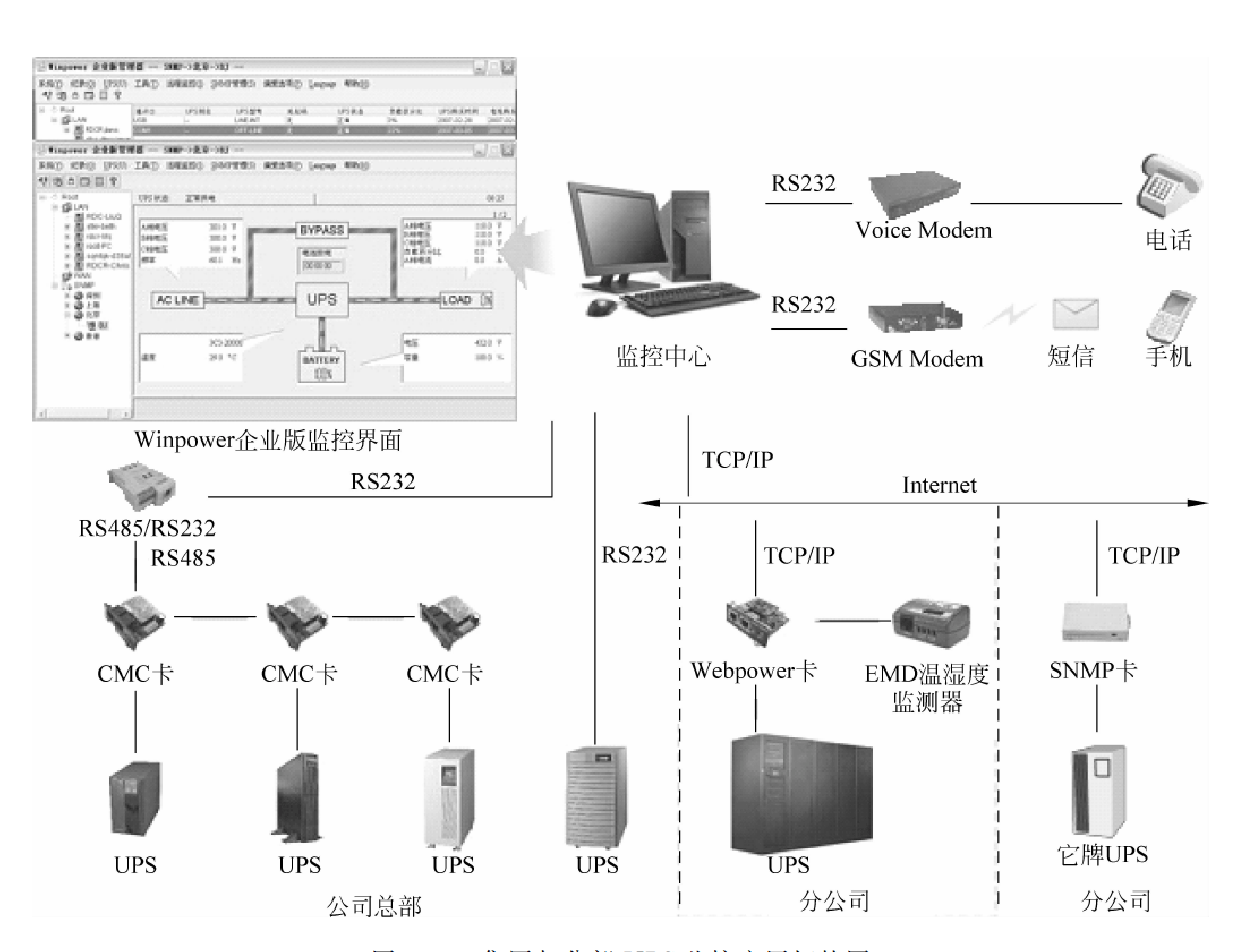


图 5-51　集团与分部 UPS 监控应用拓扑图

（3）Winpower Plus DB 监控解决方案

该方案可以对分散在局域网和广域网内多达 1000 台 UPS 进行互联网监控，数据库服务器集中保存并处理所有数据信息，不同的用户可以通过客户端软件和 Web 浏览器两种方式，以不同的权限进行访问管理。用户不仅可以实时了解 UPS 状况和及时获得通知，数据库还随时查询和提供专业的统计分析报表，预测 UPS 工作运行趋势，以便事先采取相应措施，预防电源事故的发生。如图 5-52 所示为商业银行 UPS 监控应用拓扑图。

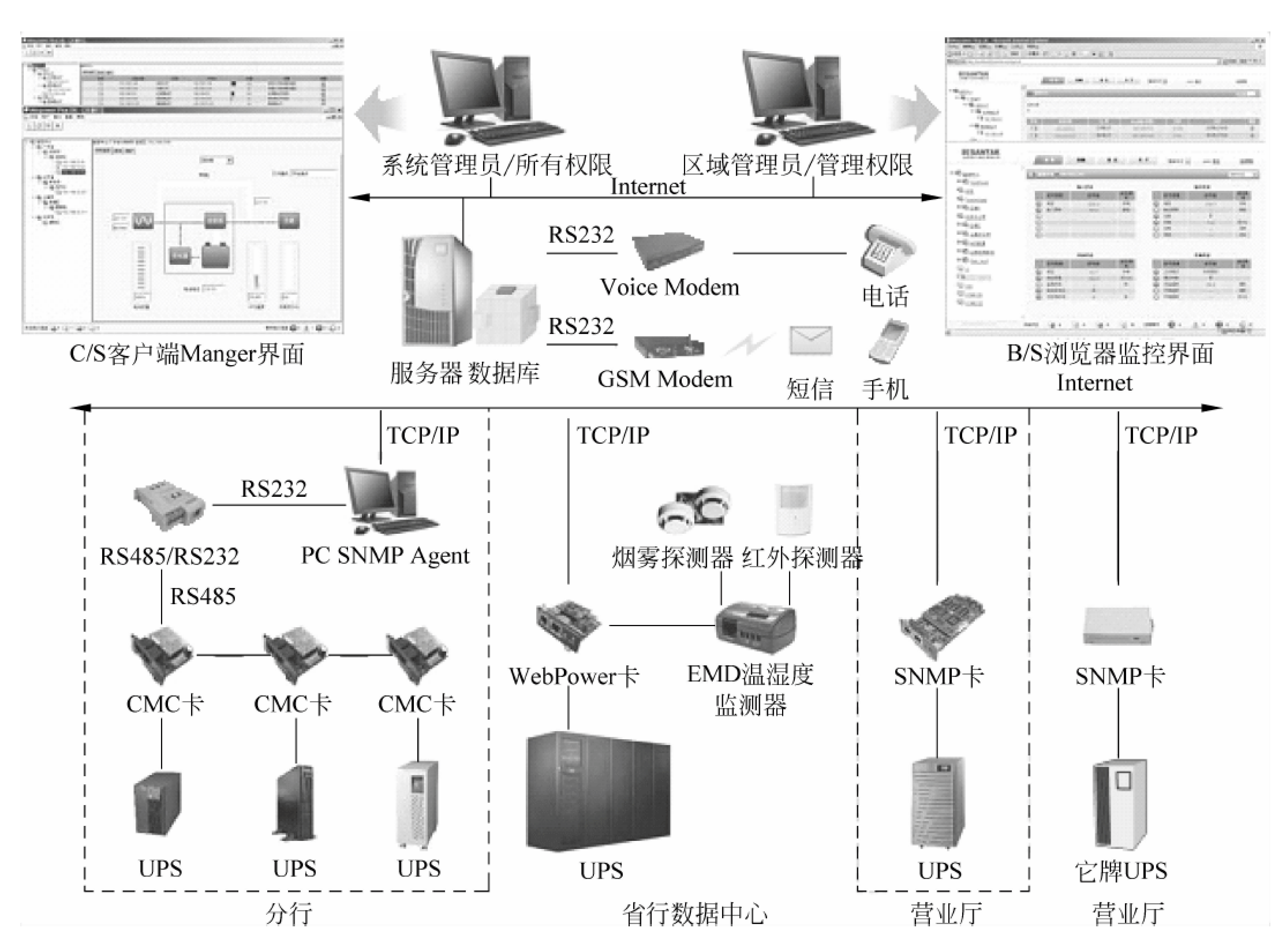


图 5-52　商业银行 UPS 监控应用拓扑图

5.5.2　UPS 管理

1. 查看 UPS 工作状态

若本机有 Agent 正在运行，当 Monitor 激活后，将直接打开“Winpower 管理器”窗口，显示本地局域网中的 Agent 及 UPS 的信息。单击左边树型结构中的项目，用户将可以得到以下信息：

- 在 LAN 网络上运行 Winpower Agent 的所有计算机。
- 连接 UPS 的串行通信口（COM 口）。
- 同 Agent 相连的 UPS 的型号。
- 用户选择的 Agent 的当前状态。

单击相应的 UPS 型号，即可显示如图 5-53 所示的 UPS 状态窗口。窗口中显示了当前 UPS 的输入与输出情况，包括电压、电流和负载百分比等状态参数。

状态图中包括 AC LINE、UPS、BATTERY、LOAD 和 BYPASS 五个部分，以及各部分电源供给方向线连接。

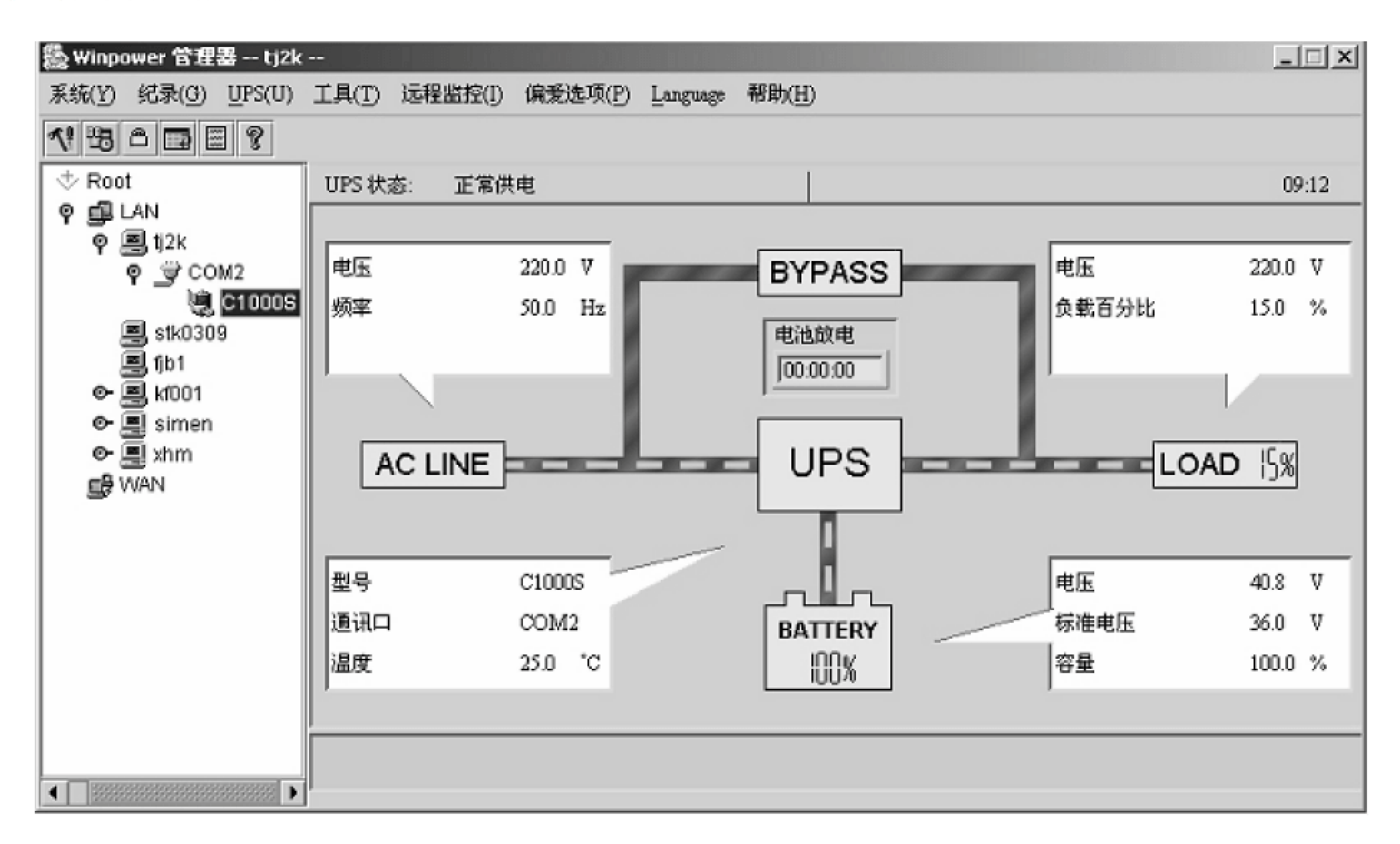


图 5-53　UPS 状态窗口

2. 事件响应设置

Winpower 可以对 UPS 事件作出响应，对于一些重大的可能影响网络正常运行的事件，不仅可以记录至日志文件，而且还可以通过邮件、手机短信等形式通知管理员。设置事件响应方式的方法为：以管理员身份登录，从主窗口的 UPS 菜单中选择“事件响应设定”后将弹出如图 5-54 所示的对话框。在“事件列表”中选择欲设置的事件，然后在右侧选中相应的响应方式复选框即可。

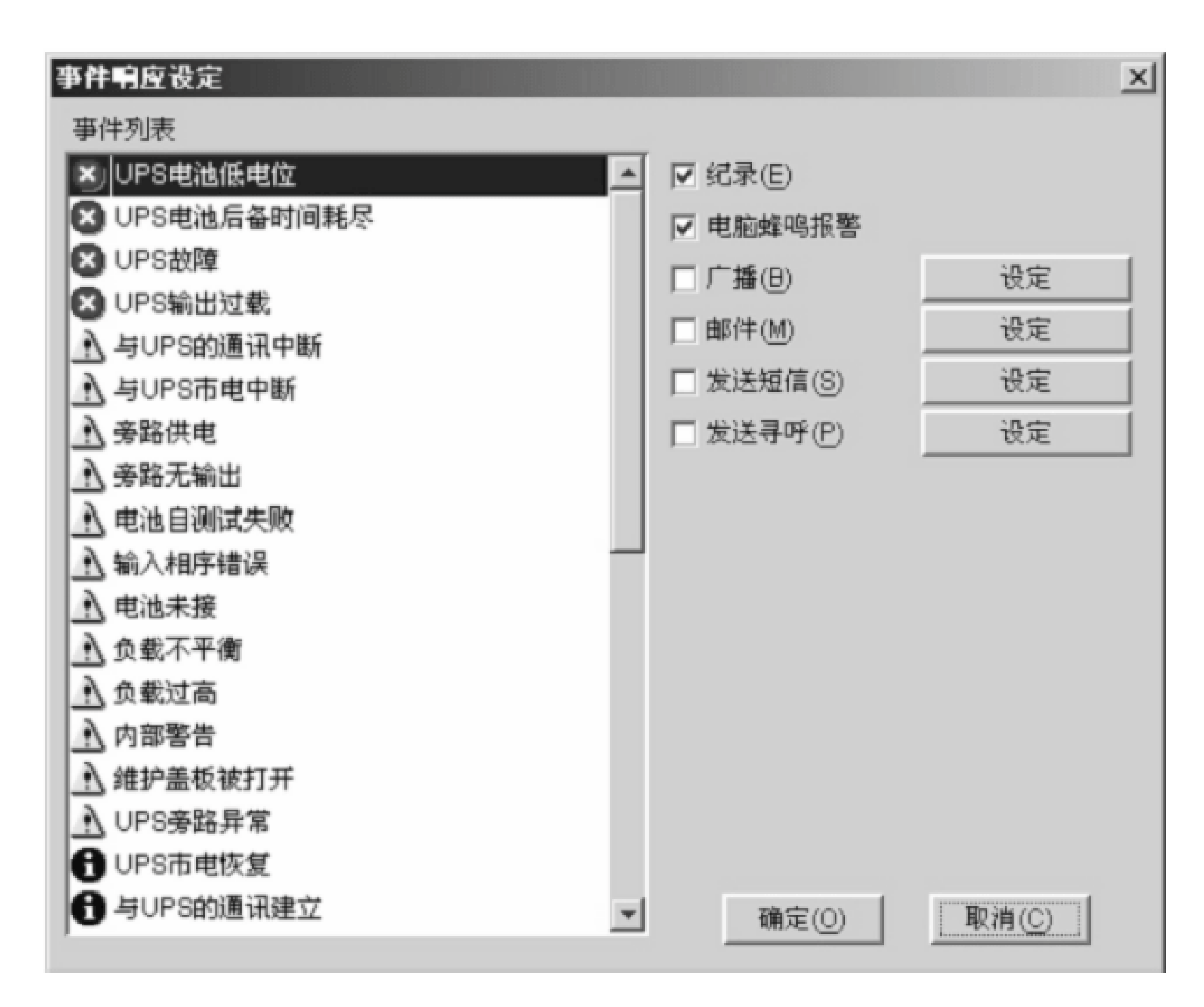


图 5-54　“事件响应设定”对话框

3. 设置关机参数

UPS 电池的容量是有限的,电池容量决定了待机的时间。因此,当停电以后应当设置合理的关机时间,并在 UPS 关机前向所有用户报警。关机参数设置方法如下:

(1) 在 UPS 菜单中选择"关机参数设定"后,弹出如图 5-55 所示的"关机参数设定"对话框。



图 5-55 "关机参数设定"对话框

(2) 根据电池数量和使用期限设置"电池备用时间",并合理设置"关闭系统所需时间"。然后,在"关机报警参数"选项区设置"关机前倒数计时报警间隔时间"和"排程关机前倒数计时报警启动时间",分别指定在关机前多长时间开始向用户报警,以及两次告警之间的时间间隔。如果需要,还可以选中"关机前执行档案"复选框,并在下面的文本框中指定在关机前执行的程序。

(3) 单击"确定"按钮,保存设置。

4. UPS 参数控制

由于市电的稳定性较差,因此,当采用旁路供电时,为了保证用电设备的正常运行,必须设置 UPS 输入、输出参数。设置的方法如下:

(1) 在 UPS 菜单中选择"UPS 控制参数"后,弹出如图 5-56 所示的"UPS 控制参数设置"对话框。

(2) 分别设置"输入频率范围"和"旁路电压范围"的上下限值,并指定各种状态下是否启用声音报警。

(3) 单击"确定"按钮,保存设置。



图 5-56 “UPS 控制参数设置”对话框

5. 自动开关机设置

Winpower 管理软件可以实现对 UPS 的自动关机和开机管理，方法如下：

(1) 在 UPS 菜单中选择“UPS 开关机排程”，弹出如图 5-57 所示的“UPS 开关机管理”对话框。

(2) 选择要设置自动开机或关机的日期，然后单击“增加 UPS 关闭”按钮，在弹出的“关闭 UPS”对话框中设置下一次关闭或启动的日期和时间。

(3) 单击“确定”按钮，保存设置。



图 5-57 “UPS 开关机管理”对话框

5.5.3 远程监控 UPS 的实现

远程监控 UPS 的方法如下：

(1) 开启允许远程监控功能：在有合法 IP 地址的计算机中启动 Winpower，在"远程监控"菜单下单击"接受远程控制"选项，如图 5-58 所示。

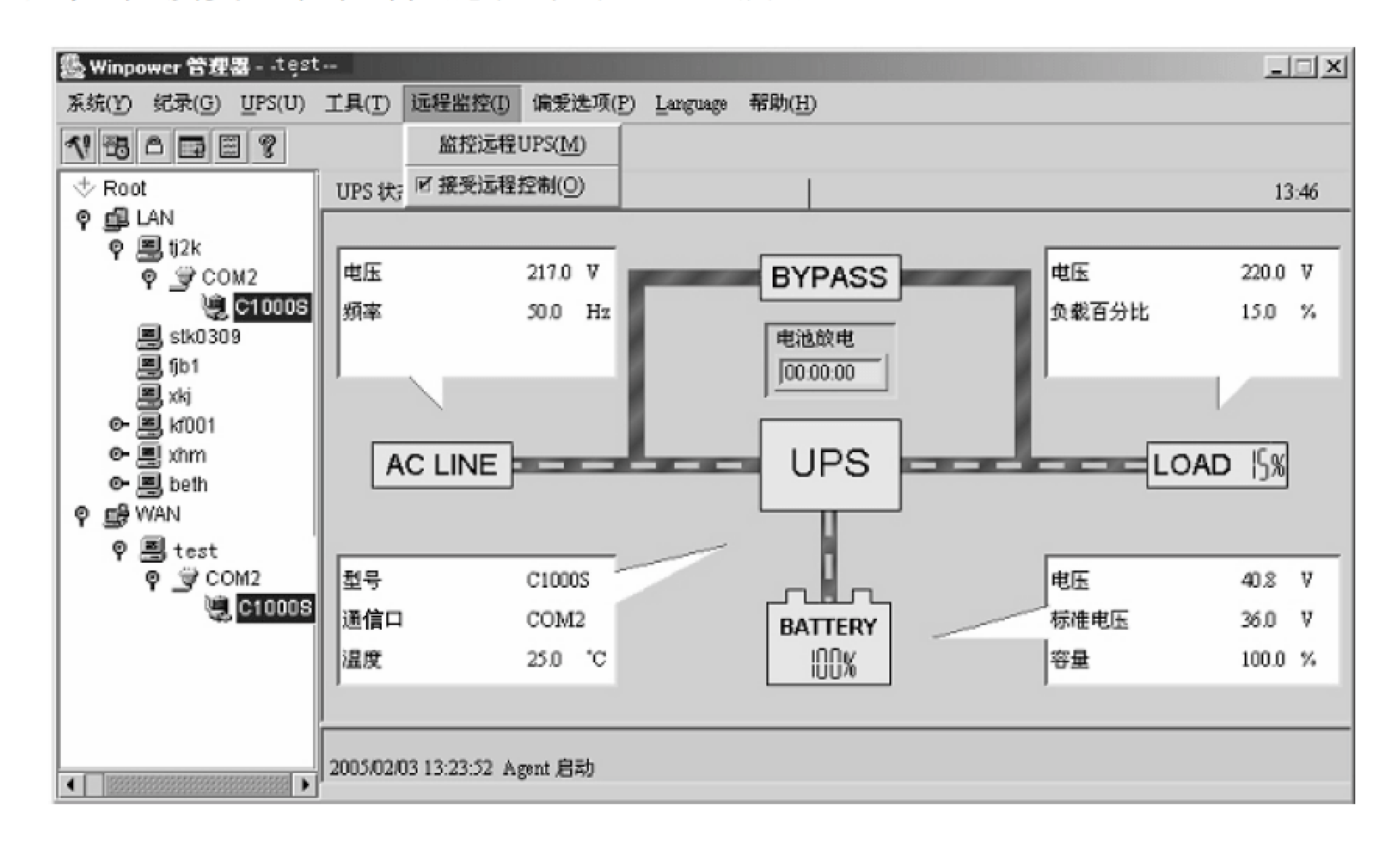


图 5-58 Winpower 管理器窗口

(2) 激活 Monitor：用鼠标右键单击桌面右下角任务栏中的电源图标，在弹出的快捷菜单中选择 Start Monitor。

(3) 选择要监控的 UPS：从"Winpower 管理器"窗口左侧的树型视图中选择 UPS，或者从"远程监控"菜单下选择"监控远程 UPS"菜单项，打开"远程监控 UPS"对话框，在弹出的对话框中输入计算机的"IP 地址"就可以在 Internet 中找到 UPS，如图 5-59 所示。

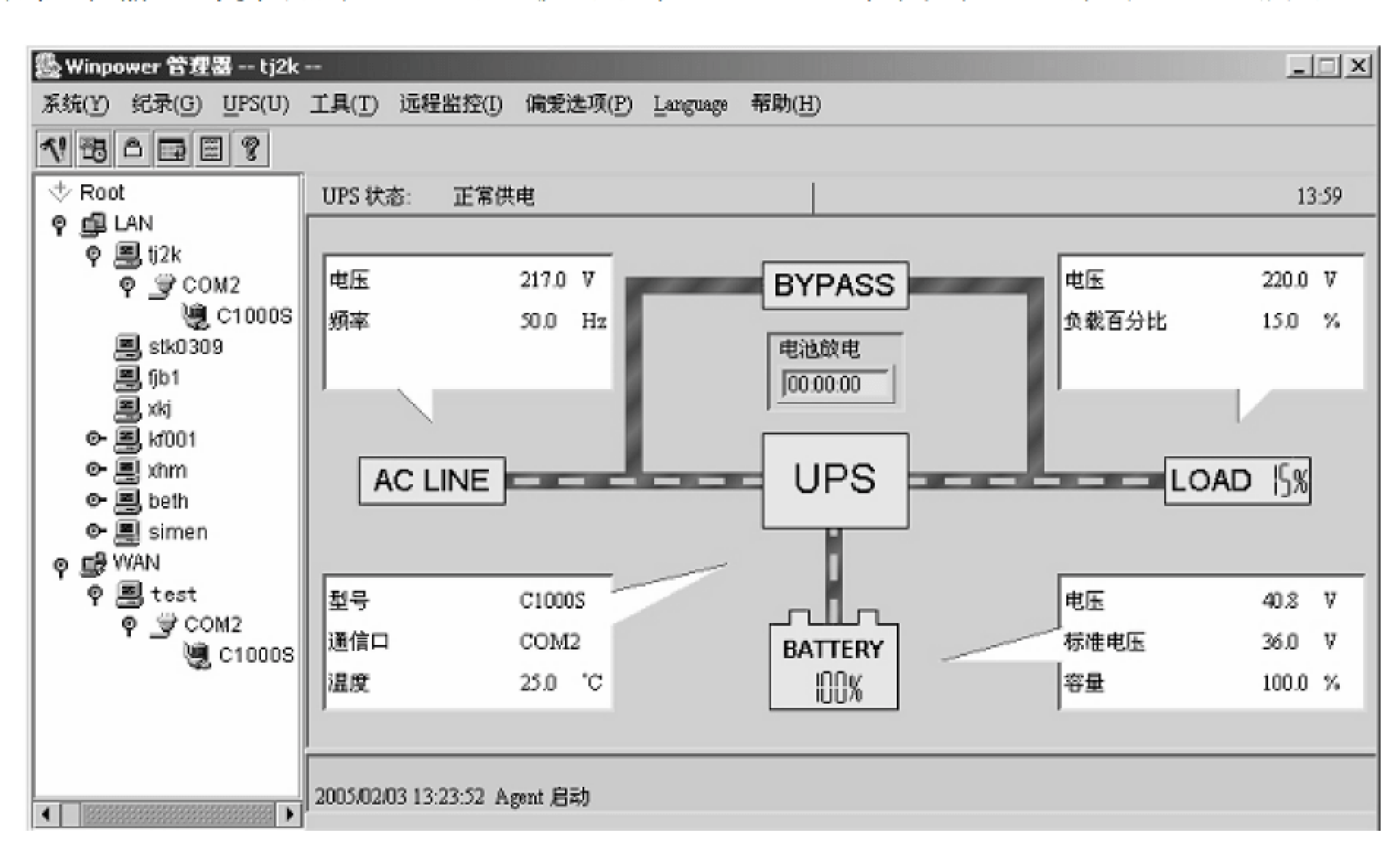


图 5-59 被监控的 UPS 信息窗口

如果此 Agent 的远程监控开关没有打开，则只能监视而不能控制。“系统”菜单的“成为系统管理员”菜单是灰色的。所以不以管理员身份登录是不能对 UPS 进行远程控制的。

5.5.4 通过网络接口管理 UPS

如图 5-60 所示，WebPower 卡是一种基于 TCP/IP、SNMP 协议，内嵌 Web 服务器的用于远程 UPS 管理的智能监控产品。用户可以通过 Web 浏览器、SNMP 网管软件或山特的 Winpower 集中监控软件来管理 UPS。WebPower 提供不同操作系统的 Shutdown 程序，Shutdown 程序运行在不同的计算机上，并且同 WebPower 进行实时的通信，当 UPS 出现异常时，Shutdown 程序可以安全关闭计算机。



图 5-60　WebPower 卡

1. 用户界面

(1) Web 浏览：通过 Web 浏览器远程获得完备的 UPS 管理信息。

(2) UPS 管理性能：Java 监视通过 Java Applets 所产生的动态图标来监控 UPS 所有的状态值(如电压、负载、电池、事件等)。

(3) SNMP 管理：Webpower 卡支持 UPS 标准的 MIB 文档(RFC1628)和企业自定义的 MIB 文档，通过网管软件获得完备的 UPS 管理性能。

2. UPS 管理

(1) 安全性管理：提供用户名和密码安全验证机制。

(2) 配置管理工具：可以设置 Webpower 网络参数、事件关机参数等。

(3) 任务调度：定期 UPS 自测，定时开关机，特别日关机功能。

(4) UPS 控制参数：为直接操作控制 UPS 提供接口。

(5) 支持串口初始化参数：支持通过串口设置 Webpower 重要参数功能，如超级用户、初始化口令、SNMP 等。

(6) 固件升级：升级方式有 Webpower 界面在线升级、运行固件升级程序、网络升级和串口升级。

(7) 监控软件集中管理：可以集中控制网络中的所有 UPS，便于用户及时发现问题，方便用户管理。

3. 诊断

(1) UPS 定期自测：通过周期性测试 UPS，可以及时发现电源问题。

(2) UPS 电池测试：通过 UPS 自测试了解电池状况，以便采取预防措施。

(3) 数据记录：通过查看 Webpower 的历史记录数据，了解 UPS 的工作状况，便于系统管理员更好地掌握 Webpower 的工作状况。

4. 事件管理

支持 SNMPTrap，Webpower 支持多种电源和环境事件实时警报，可以通过 SNMP Trap 机制和 E-mail 第一时间获知发生的事件。

5. 关机/启动

(1) 关闭操作系统：通过 Webpower Shutdown 程序，可以安全关闭用户系统。

(2) 关闭多服务器：通过 TCP/IP 网络，可以关闭多台服务器(多达 250 台)。

(3) 开启/关闭 UPS：可以直接关闭或开启连接设备的 UPS，便于客户进行系统设备维护。

(4) 网络唤醒：当关机事件消失，UPS 恢复正常时，可以通过网络将关机的计算机开机。

5.6 WLAN 管理

5.6.1 WLAN 概述

1. WLAN 的概念

无线局域网(Wireless Local Area Network，WLAN)是一种无线数据网络，它是以无线方式构建的局域网。终端用户无须使用线缆，只要通过射频介质与无线接入点(AP)建立连接即可上网，WLAN 给移动用户带来了极大的便利。

2. WLAN 网络架构

在 WLAN 技术应用中，可以将 WLAN 网络架构分为两种：①"胖" AP 网络架构，AP 可以自行控制接入的无线用户端，并实施相应的管理策略；②"瘦"AP 网络架构，由接入控制器(Access Control，AC)通过有线网络集中控制下联 AP，AP 通过加入 AC 创建的 AP 组与 AC 关联，无线用户通过接入 AP 实现与网络通信，如图 5-61 所示。

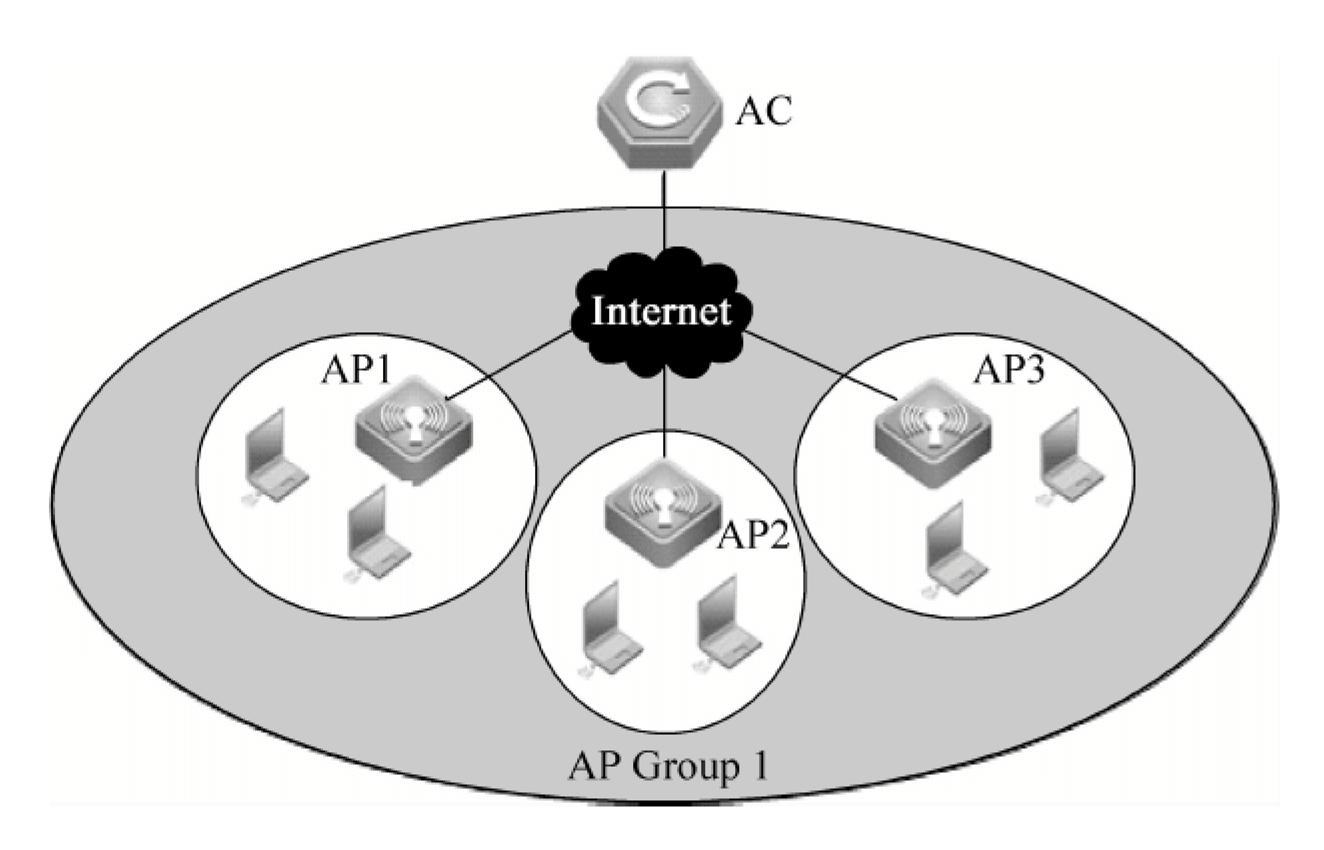


图 5-61 "瘦"AP 网络拓扑示意图

3. WLAN 管理的应用

在"瘦"AP 网络架构中，AC 通过 WLAN 管理对无线网络进行规划部署，确保网络高效稳定地运行。WLAN 管理可以将无线网络划分成多个 WLAN 子网，并根据各子网的服务性质实施相应的管理策略，无线用户通过加入不同的 WLAN 子网可获得不同的网络服务。

5.6.2 配置 WLAN 管理

用户可以在 AC 上创建多个 WLAN，并进入指定 WLAN 的配置模式，根据实际网络需要配置该 WLAN 的相关功能属性。本节以锐捷产品的 WLAN 技术为例，介绍一些常用的基本配置与管理命令。

1. 创建 WLAN

在无线网络中,用户可以通过创建 WLAN 将网络划分成多个 WLAN 子网,并在 WLAN 配置模式下配置 WLAN 子网的功能属性,为无线用户提供不同的网络服务。

在创建 WLAN 的同时必须关联一个服务组织标识码(Service Set Identifier,SSID),SSID 仅是一个网络服务域的名称,一个 SSID 可以对应一个或多个 WLAN。如图 5-62 所示,创建的 WLAN 1、WLAN 2、WLAN 3 分别对应同一个 SSID 为"Corporation"的网络服务域,在这个网络服务域中,User A、User B、User C 分别属于不同的 WLAN 子网。

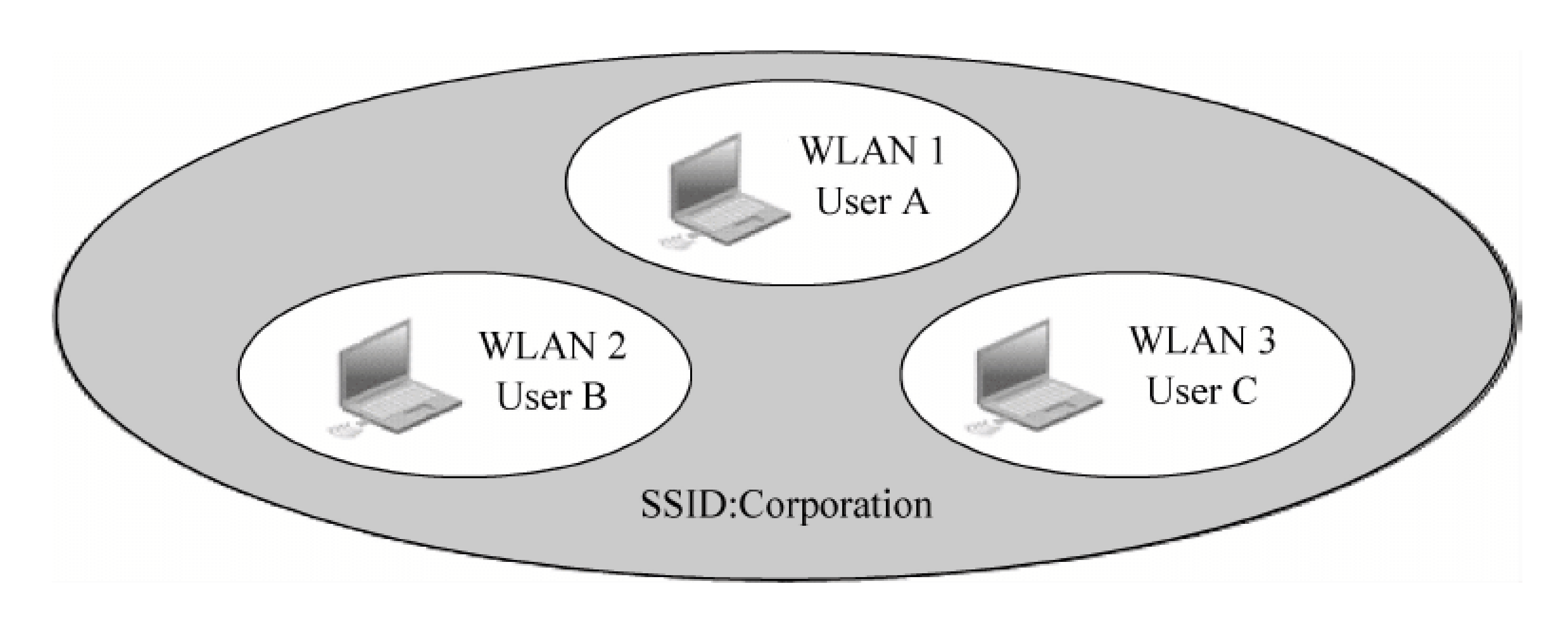


图 5-62 WLAN 子网示意图

在 AC 上创建 WLAN 的配置命令如表 5-15 所示。

表 5-15 WLAN 的配置命令表

命令	作用
Ruijie (config) # [no] wlan-config wlan-id [profile-string] [ssid-string]	创建 WLAN 以及进入指定 WLAN 的配置模式。 wlan-id:指定 WLAN 的 ID 号,取值范围 1~4 094; profile-string:该 WLAN 的描述符,可省略; ssid-string:SSID 标识符,创建 WLAN 的同时,必须指定该 WLAN 关联的 SSID; 使用 no 选项可以删除指定的 WLAN
Ruijie (config) # show wlan-config summary	查看 AC 上的 WLAN 配置列表

2. 禁止 SSID 广播

在 WLAN 网络中,AP 会定期广播 SSID 信息,向外通告无线网络的存在,无线用户通过使用无线网卡搜索 SSID 发现网络。为避免无线网络被非法用户通过 SSID 广播搜索到,并建立非法连接,可以将 SSID 广播禁用,禁用 SSID 广播的配置命令如表 5-16 所示。

表 5-16 禁用 SSID 配置表

命令	作用
Ruijie (config) # wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan) # [no] enable-broad-ssid	默认情况下,SSID 广播为"enable",使用 no 选项可以禁止 SSID 广播
Ruijie (config-wlan) # show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

3. 配置 Tunnel 模式

在 WLAN 网络中，AC 通过无线接入点控制与供应协议(Controlling and Provisioning of Wireless Access Point，CAPWAP)控制管理下联的 AP，CAPWAP 为 AC 和 AP 之间提供通信隧道。AP 可以将收到的无线数据直接在本地转发，或封装成 802.3 帧格式转发给 AC。用户可以在 WLAN 中配置 Tunnel 模式来指定 AP 转发无线数据的方式，Tunnel 模式的配置命令如表 5-17 所示。

表 5-17　Tunnel 配置命令表

命　　令	作　　用
Ruijie (config)# wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan)# tunnel { 8023 | local }	配置 Tunnel 模式： • 8023：AP 将收到的无线数据封装成 802.3 帧格式转发给 AC。 • local：AP 将收到的无线数据直接在本地转发默认情况下，Tunnel 模式为 local
Ruijie (config-wlan)# no tunnel	恢复至默认配置
Ruijie (config-wlan)# show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

4. 配置短前导码

前导码(Preamble)是数据帧头部的一组 Bit 位，用于同步发送端与接收端的传输信号。前导码分为两种：长前导码(Long Preamble)和短前导码(Short Preamble)。默认情况下，设备选择长前导码传输数据。为了提高网络传输效率，用户可以使用短前导码，短前导码配置的命令如表 5-18 所示。

表 5-18　Short Preamble 配置命令表

命　　令	作　　用
Ruijie (config)# wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan)#[no] short-preamble	使用短前导码。默认为 disable，即使用长前导码；使用 no 选项可以恢复默认配置
Ruijie (config-wlan)# show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

5. 配置 RTS Threshold

为了避免信道冲突而导致数据传输失败，IEEE 802.11 MAC 协议提供了一个 RTS/CTS(Request To Send/Clear To Send)握手协议，即请求发送/允许发送协议。如果每个工作站每次发送数据前都要执行 RTS/CTS 握手，将导致过多的 RTS 帧占用信道带宽，可以设置 RTS Threshold 来指定发送数据的帧长度，如果帧长度小于 RTS Threshold 设置的门限，将不执行 RST/CTS 握手，RTS Threshold 配置的命令如表 5-19 所示。

表 5-19　RTS Threshold 配置命令表

命　　令	作　　用
Ruijie (config)# wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan)# rts-threshold threshold	配置 RTS Threshold。其中，threshold 指定数据的帧长度，取值范围为 257～2 347，默认值为 2 347
Ruijie (config-wlan)# no rts-threshold	恢复至默认配置
Ruijie (config-wlan)# show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

6. 配置短时隙

在 WLAN 网络中，为避免多个工作站发送数据引起信道竞争，工作站在发送数据之前需要检测信道是否空闲。如果检测到信道处于空闲状态，工作站并不立即发送数据，而是等待一个退避时间(Backoff Time)。退避时间是时隙时间(Slot Time，MAC 协议中的一个操作时间单元)的随机整数倍，假设随机值为 3，则每经过一个时隙时间，系统自动将数值减 1，待数值减为零时，工作站开始发送数据。因此，降低时隙时间可以减少总体退避时间，从而增加网络的吞吐量。

用户可以指定 WLAN 使用短时隙，即将时隙时间从标准的 20μs 降低至 9μs，配置短时隙的命令如表 5-20 所示。

表 5-20　Short Slot Time 配置命令表

命　　令	作　　用
Ruijie (config)# wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan)# [no] short-slot-time	使用短时隙，默认情况下，短时隙为"disable"。使用 no 选项可以禁用短时隙
Ruijie (config-wlan)# show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

7. 配置数据帧重传次数

在 WLAN 网络中，如果发送方传输数据失败，可以尝试重新传输。基于 RTS Threshold 门限值可以将数据帧分为长数据帧和短数据帧，并根据数据帧长短设置对应的重传次数。

(1) 配置长数据帧重传次数

配置长数据帧重传次数的命令如表 5-21 所示。

表 5-21　配置长数据帧重传次数命令表

命　　令	作　　用
Ruijie (config)# wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan)# long-retries count	配置长数据帧重传次数。其中，count 指重传次数，取值范围为 1～4，默认值为 4
Ruijie (config-wlan)# no long-retries	恢复默认配置
Ruijie (config-wlan)# show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

(2) 配置短数据帧重传次数

配置短数据帧重传次数的命令如表 5-22 所示。

表 5-22 配置短数据帧重传次数命令表

命　　令	作　　用
Ruijie (config) # wlan-config wlan-id	进入指定 WLAN
Ruijie (config-wlan) # short-retries count	配置短数据帧重传次数。其中,count 指重传次数,取值范围为 1～7,默认值为 7
Ruijie (config-wlan) # no short-retries	恢复默认配置
Ruijie (config-wlan) # show *nalw*-config cb wlan-id	查看指定 WLAN 的配置信息

5.6.3 AP 管理配置

1. AP 管理概述

早期的 WLAN 网络是采用有线交换机+胖 AP 的组网方式。因此,在 WLAN 网络部署中需要对胖 AP 进行逐一配置。随着网络规模的不断扩大,原有的胖 AP 无线技术已无法适应现有的网络发展需要。

(1) 瘦 AP 技术

瘦 AP 无线技术是采用有线交换机+无线控制器+瘦 AP 的组网方式,即 AP 作为简单的无线接入点,不具备管理控制功能,而通过无线控制器统一管理所有 AP,向指定 AP 下发控制策略,无须在各 AP 上单独配置,如图 5-63 所示。AC 通过有线网络与多个 AP 相连,用户只需在 AC 上对所关联的 AP 进行配置管理。

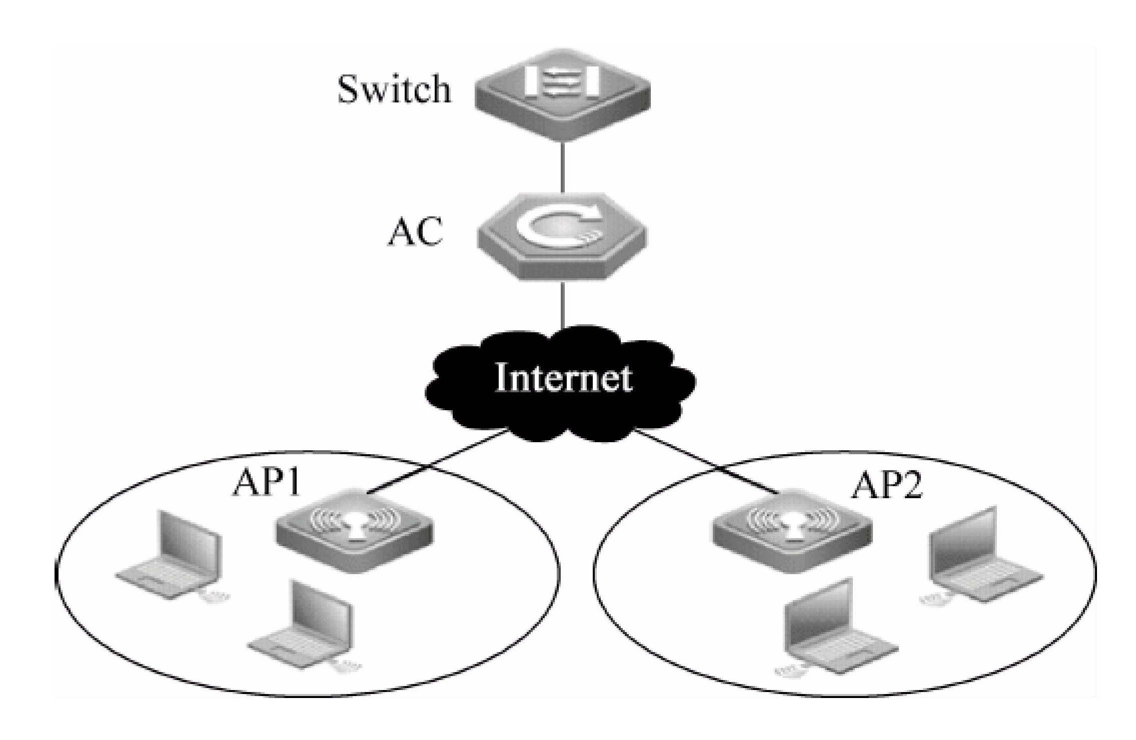


图 5-63 简单瘦 AP 组网拓扑

(2) AP 管理的工作原理

AP 管理是通过在 AC 和 AP 之间运行 CAPWAP 协议实现的,CAPWAP 在 AC 和 AP 之间提供通信隧道,负责封装 AC 发往 AP 的控制报文,以及 AP 发往 AC 的数据报文。

AP 管理是指用户在 AC 上进行相应的配置,并封装成相应的 CAPWAP 控制报文,通过 CAPWAP 控制通道传输至 AP 进行解析并执行的过程。

2. AP 管理的配置模式

在 WLAN 网络中,对瘦 AP 的控制管理统一集中在 AC 上配置,用户可以通过 AC 的控制台进入多个配置模式来配置管理 AC 和 AP。AP 管理具有以下 3 种模式:

(1) AC 配置模式：在该模式下可以对 AC 自身的功能属性以及指定 AP 的部分功能属性进行配置。

(2) AP 组配置模式：在该模式下可以对指定 AP 组的功能属性进行配置。在该配置模式下的配置会对该 AP 组内的所有 AP 生效。

(3) AP 配置模式：在该模式下可以对指定 AP 的功能属性进行配置。在该配置模式下的配置不会影响其他 AP。

3. 配置 AP 管理

1) AC 配置模式的管理命令

(1) 进入 AC 配置模式

进入 AC 配置模式的命令如表 5-23 所示。

表 5-23 进入 AC 配置模式命令表

命　令	作　用
Ruijie (config)# ac-controller Ruijie (config-ac)#	进入 AC 命令模式

(2) 配置 AC 的名称

为方便用户在 WLAN 网络中识别管理 AC，可以为不同的 AC 配置不同的名称。在 AC 配置模式下，配置 AC 的名称的命令如表 5-24 所示。

表 5-24 配置 AC 名称命令表

命　令	作　用
Ruijie (config-ac)# ac-name ac-name	配置 AC 的名称。其中，ac-name：配置该 AC 的名称描述符，最多可配置 64 个字符，不能包含空格
Ruijie (config-ac)# no ac-name	恢复至默认配置
Ruijie (config-ac)# exit	如果需要查看配置结果，则执行此命令退出 AC 配置模式
Ruijie (config)# show ac-config	查看配置的 AC 名称

(3) 配置 AC 可以连接的最大 AP 数

在 WLAN 网络中，一台 AC 可以连接多台 AP。用户可以配置指定 AC 可连接的最大 AP 数。在 AC 配置模式下，配置 AC 可以连接的最大 AP 数的命令如表 5-25 所示。

表 5-25 配置最大 AP 数命令表

命　令	作　用
Ruijie (config-ac)# wtp-limit max-num	配置该 AC 可以连接的最大 AP 数。其中，max-num 指可连接的最大 AP 数，WS5302 的取值范围为 1～64，默认值为 8；WS5708 的取值范围为 1～768，默认值为 128
Ruijie (config-ac)# no wtp-limit	恢复至默认配置
Ruijie (config-ac)# exit	如果需要查看配置结果，请执行此命令退出 AC 配置模式
Ruijie(config-ac)# show ac-config	查看配置信息

(4) 配置 AC 可以连接的最大无线用户数

在 WLAN 网络中，一台 AC 可以连接多台 AP，一台 AP 又可以连接多个无线用户。用户可以配置指定 AC 服务范围内最多可连接的无线用户数。在 AC 配置模式下，配置 AC

可以连接的最大无线用户数的命令如表 5-26 所示。

表 5-26　配置 AC 可连接的最大用户数命令表

命　　令	作　　用
Ruijie (config-ac) # sta-limit max-num	配置 AC 可以连接的最大无线用户数。其中，max-num 指可连接的最大无线用户数，WS5302 的取值范围为 1～24 000，默认值为 2 010；WS5708 的取值范围为 1～196 608，默认值为 32 768
Ruijie (config-ac) # no sta-limit	恢复至默认配置
Ruijie (config-ac) # exit	如果需要查看配置结果，则执行此命令退出 AC 配置模式
Ruijie (config-ac) # show ac-config	查看配置信息

2）AP 组配置模式的管理命令

AP 在 WLAN 网络中要能为无线用户提供服务，必须与某个 AC 建立连接，并且需要加入一个 AP 组。所有新加入的 AP 都属于默认 AP 组 default。默认 AP 组不可创建，不可删除。用户可以创建自定义的 AP 组，并在该 AP 组配置模式下设置相关功能属性。

（1）创建 AP 组

在配置模式下创建 AP 组的命令如表 5-27 所示。

表 5-27　创建 AP 组命令表

命　　令	作　　用
Ruijie (config) # [no] ap-group test-group	创建 AP 组。其中，test-group 指 AP 组名。使用 no 选项可以删除该 AP 组

（2）配置指定 AP 组的 WLAN-CVI 映射

在 WLAN 网络中，AP 为无线用户提供射频服务需要先加入一个特定的 WLAN。可以在 AC 上创建多个 WLAN，将各 AP 组划分到对应的 WLAN，AP 通过加入指定的 AP 组与对应的 WLAN 建立关联，并基于该 WLAN 为无线用户提供服务。

为实现无线网络与有线网络之间通信，用户需要配置指定 WLAN 与 VLAN 的三层虚拟接口(CVI)绑定。配置指定 AP 组的 WLAN-CVI 映射的命令如表 5-28 所示。

表 5-28　配置 WLAN-CVI 映射命令表

命　　令	作　　用
Ruijie (config) # ap-group test-group	进入指定的 AP 组
Ruijie (config-ap-group) # [no] interface-mapping wlan-id vlan-id [radio radio-id]	配置指定的 AP 组的 WLAN-VLAN 映射。其中，wlan-id 指指定的 WLAN，该 WLAN 必须已经创建，取值范围为 1～2 010； vlan-id：指定的 VLAN，该 VLAN 的 CVI 已创建，取值范围为 1～4 094； radio-id：指定 AP 的 Radio，若不指定 radio-id 参数，会应用到 AP 组内的所有 AP 的所有 radio 上
Ruijie (config-ap-group) # exit	如果需要查看配置结果，则执行此命令退出 AP 组配置模式
Ruijie (config) # show ap-group intf-wlan-map test-group	查看指定 AP 组的 wlan-vlan 映射表

(3) 配置指定 AP 组内的 AP 可连接的最大无线用户数

在 WLAN 网络中,可以指定 AP 组内的所有 AP 可连接的最大无线用户数,配置指定 AP 组内的 AP 可连接的最大无线用户数的命令如表 5-29 所示。

表 5-29　指定 AP 组内可连接的最大用户数命令表

命　　令	作　　用
Ruijie (config)# ap-group test-group	进入指定的 AP 组
Ruijie (config-ap-group)# sta-limit max-num	配置指定 AP 组内的所有 AP 可连接的最大无线用户数。其中,max-num 指可支持的最大用户数,取值范围为 1～256
Ruijie (config-ap-group)# no sta-limit	使用 no 选项可恢复至默认值

(4) 配置指定 AP 组内所有 AP 的用户名和密码

为避免非法用户通过 Telnet 直接登录到 AP 上对其实施配置控制,影响正常 WLAN 网络运行,用户可以配置指定 AP 组的用户名和密码,该 AP 组内的所有 AP 统一使用该用户名和密码,配置命令如表 5-30 所示。

表 5-30　为 AP 组指定用户名和密码命令表

命　　令	作　　用
Ruijie (config)#ap-group test-group	进入指定的 AP 组。其中,test-group 为指定的 AP 组名称
Ruijie (config-ap-group)# [no] credentialuser-name password	配置指定 AP 组的用户名和密码。其中,user-name 指用户名; password 指密码; 使用 no 选项,取消该配置

(5) 配置指定 AP 组同步 AC 的时间

用户可以指定 AP 组内的所有 AP 同步 AC 的时间,配置命令如表 5-31 所示。

表 5-31　配置同步 AC 时间命令表

命　　令	作　　用
Ruijie (config)#ap-group test-group	进入指定的 AP 组。test-group 为指定的 AP 组名称
Ruijie (config-ap-group)# timestamp	配置指定 AP 组同步本 AC 的时间

(6) 配置检测指定 AP 组内 AP 与 AC 之间的链路状态

在 WLAN 网络中,AP 可以定期发送报文给 AC,AC 通过接收 AP 发送的报文,统计该报文的传输延迟,管理员通过查看相应的延迟时间,定位 AC 与 AP 之间的链路状态。可以在指定 AP 组的配置模式下,开启检测 AC 与指定 AP 组内所有 AP 之间的链路状态的功能。配置命令如表 5-32 所示。

表 5-32　配置链路状态命令表

命　　令	作　　用
Ruijie (config)#ap-group test-group	进入指定的 AP 组。test-group 为指定的 AP 组名称
Ruijie (config-ap-group)# [no] link-latency	配置检测 AC 与指定 AP 组内 AP 之间的链路状态。默认情况下,未开启检测链路状态。使用 no 选项可恢复至默认配置

续表

命　　令	作　　用
Ruijie (config-ap-group)＃ exit	如果需要查看 AC 与 AP 之间的链路状态信息，请执行此命令退出 AP 组配置模式
Ruijie (config)＃ show ap-config link-latency {all | single ap-name}	查看 AC 与 AP 之间的链路状态信息。其中，all 指查看与 AC 关联的所有 AP 的链路状态信息；single ap-name 指查看单个 AP 的链路状态信息

3）AP 配置模式的管理命令

如果用户需要对特定的 AP 实施管理配置，可以在 AC 上配置进入指定 AP 的配置模式，并在该配置模式下执行如下配置。

(1) 配置 AP 所属的 AP 组

所有新加入的 AP 都属于默认 AP 组 default。用户可以将指定 AP 加入自行创建的 AP 组，配置命令如表 5-33 所示。

表 5-33　配置 AP 组命令表

命　　令	作　　用
Ruijie (config)＃ ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)＃[no] ap-group test-group	配置 AP 所属的 AP 组。其中，test-group 为指定的 AP 组名。使用 no 选项，取消 AP 所属组，恢复至默认 AP 组
Ruijie (config-ap)＃ exit	如果需要查看配置结果，请执行此命令退出 AP 配置模式
Ruijie (config-)＃ show ap-config cb ap-name	查看指定 AP 的状态信息

(2) 配置 AP 的名称

一旦 AP 与 AC 关联，AC 自动为 AP 按数字排序方式命名(例如 AP-0001)。为方便用户识别管理，可以自行为 AP 重新命名，配置 AP 名称的命令如表 5-34 所示。

表 5-34　配置 AP 名称命令表

命　　令	作　　用
Ruijie (config)＃ ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)＃ ap-name name	配置 AP 的名称。其中，name 为配置 AP 的名称描述符，不能带空格
Ruijie (config-ap)＃ exit	如果需要查看配置结果，请执行此命令退出 AP 配置模式
Ruijie (config)＃ show ap-config inventory ap-name	查看指定 AP 的名称

(3) 配置指定 AP 的频段

目前 AP 可支持 2.4GHz 和 5GHz 两个频段的射频传输，用户可以指定 AP 的射频支持的频段，配置命令如表 5-35 所示。

表 5-35　配置 AP 频段命令表

命　　令	作　　用
Ruijie (config)＃ ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)＃ radio-type radio-id {802.11a | 802.11b}	配置指定 AP 的 Radio 频段。其中，radio-id 为指定射频号。802.11a 支持 5GHz 的频段；802.11b 支持 2.4GHz 的频段。默认情况下，单频 AP(即 Radio 1)支持 2.4GHz 频段，双频 AP 的 Radio 1 支持 2.4GHz，Radio 2 支持 5GHz
Ruijie (config-ap)＃ exit	如果需要查看配置结果，请执行此命令退出 AP 配置模式
Ruijie (config)＃ show ap-config radio radio-id status ap-name	查看指定 AP 指定 radio 的配置信息

(4) 配置 AP 的无线信道

无线信道(Channel)是 AP 与无线用户之间传输射频介质的通道。不同的国家以及不同的频段支持的信道也不同。在中国，2.4GHz 的频段可以配置的信道有 13 个(channel 1、2、3、…、13)，5GHz 的频段可以配置的信道有 5 个(channel 149、153、157、161、165)。在 2.4GHz 的频段中，互相重叠的信道会产生干扰，为避免无线信号冲突，建议将其配置为不重叠的信道(例如 channel 1、6、11)；而 5GHz 的频段，这 5 个信道不会互相重叠，也不会产生干扰。

用户可以配置指定 AP 的信道，配置命令如表 5-36 所示。

表 5-36　配置 AP 信道命令表

命　　令	作　　用
Ruijie (config)＃ ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)＃ channel channel-id radio radio-id	配置指定 AP 的信道。其中，channel-id 为指定 AP 使用的信道，不同的频段，信道取值范围不同。如果国家码为"CN"，2.4GHz 的频段下可配置的 channel 为 1～13 个；5GHz 的频段下可配置的 channel 为 149、153、157、161、165。radio-id 为指定射频号
Ruijie (config-ap)＃ exit	如果需要查看配置结果，请执行此命令退出 AP 配置模式
Ruijie (config)＃ show ap-config radio radio-id config ap-name	查看指定 AP 指定 radio 的信道配置信息

(5) 配置指定 AP 可连接的最大无线用户数

在 WLAN 网络中，一台 AP 可连接多个无线用户数，管理员可以配置指定 AP 可连接的最大用户数，配置命令如表 5-37 所示。

表 5-37 配置 AP 可连接的最大用户数命令表

命 令	作 用
Ruijie (config)# ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)# sta-limit max-num	配置指定 AP 可连接的最大用户数。其中,max-num 为可支持的最大用户数,取值范围为 1～32,默认值为 32
Ruijie (config-ap)# no sta-limit	使用 no 选项恢复至默认值
Ruijie (config-ap)# exit	如果需要查看配置结果,请执行此命令退出 AP 配置模式
Ruijie (config)# show ap-config cb ap-name	查看指定 AP 的状态信息

(6) 配置指定 AP 的用户名和密码

为避免非法用户通过 Telnet 直接登录到 AP 上对其实施配置控制,影响正常 WLAN 网络运行,用户可以配置指定 AP 的用户名和密码,配置命令如表 5-38 所示。

表 5-38 配置 AP 用户名和密码命令表

命 令	作 用
Ruijie (config)# ap-config ap-name	进入指定 AP 的配置模式
Ruijie (config-ap)# [no] credential user-name password	配置指定 AP 的用户名和密码。其中,user-name 为用户名;password 为密码。使用 no 选项,取消该配置

(7) 配置为指定 AP 升级版本

用户可以单独为指定的 AP 进行版本升级,配置命令如表 5-39 所示。

表 5-39 配置 AP 升级命令表

命 令	作 用
Ruijie(config)# ap-config ap-name	进入指定 AP 的配置模式
Ruijie(config-ap)# ap-image-id ap. bin	配置为指定 AP 升级版本。其中,ap. bin 为软件版本文件
Ruijie(config-ap)# show ap-config cb ap-name	查看指定 AP 的状态信息

5.6.4 WLAN 配置案例

1. 组网拓扑

如图 5-64 所示,一台 AC 直连四台 AP:AP0001、AP0002、AP0003、AP0004,产品型号为 AP220-E 或 AP220-SE。

2. 应用需求

(1) 建立基本的 AP 管理:将 AP 加入 AC,由 AC 为接入 AP 同步升级版本,无线用户通过接入 AP 实现与有线网络通信。

(2) 建立安全的 AP 管理:过滤非法无线用户;防止非法用户对 AP 自行配置。

3. 配置要点

根据以上需求配置如下:

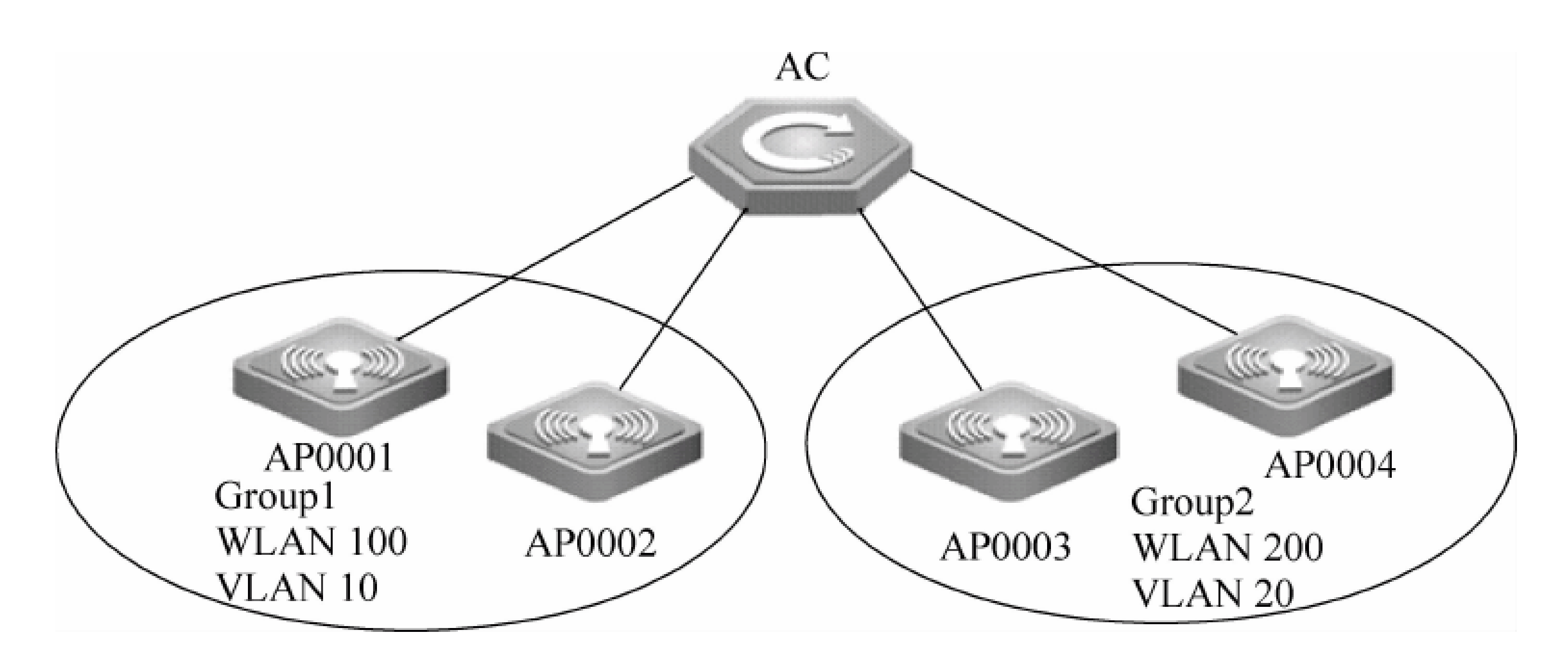


图 5-64　AP 直连 AC 的拓扑示意图

(1) 配置指定 AP 组的 WLAN-CVI 映射，配置 AP 所属的 AP 组，并配置 AC 为指定的 AP 系列升级版本。

(2) 配置 AC 网络中的无线用户黑名单，配置指定 AP 的用户名和密码。

4. 配置步骤

(1) 配置指定 AP 组的 WLAN-CVI 映射。

```
!创建 VLAN 10、VLAN20，并配置对应的 CVI。
Ruijie (config)# vlan 10
Ruijie (config-vlan)# int vlan 10
Ruijie (config-if-VLAN 10)# exit
Ruijie (config)# vlan 20
Ruijie (config-vlan)# int vlan 20
Ruijie (config-if-VLAN 10)# exit
!创建 WLAN 100、WLAN200.
Ruijie (config)#wlan-config 100 pro-100 ssid-100
Ruijie (config-wlan)#exit
Ruijie (config)#wlan-config 200 pro-200 ssid-100
Ruijie (config-wlan)#exit
!创建 AP 组 Group 1、Group 2，在对应的 AP 组内配置指定 WLAN 和 CVI 的映射。
Ruijie (config)#ap-group group1
Ruijie (config-ap-group)#interface-mapping 100 10
Ruijie (config-ap-group)#exit
Ruijie (config)#ap-group group2
Ruijie (config-ap-group)#interface-mapping 200 20
Ruijie (config-ap-group)#exit
```

(2) 配置 AP 所属的 AP 组

```
!指定 AP0001、AP0002 加入 group1，AP0003、AP0004 加入 group2。
Ruijie (config)# ap-config AP0001
Ruijie (config-ap)# ap-group group1
Ruijie (config-ap)# exit
Ruijie (config)# ap-config AP0002
Ruijie (config-ap)# ap-group group1
Ruijie (config-ap)# exit
Ruijie (config)# ap-config AP0003
Ruijie (config-ap)# ap-group group2
```

```
Ruijie (config-ap)# exit
Ruijie (config)# ap-config AP0004
Ruijie (config-ap)# ap-group group2
Ruijie (config-ap)# exit
```

(3) 配置 AC 为指定的 AP 升级版本

```
!进入 AC 配置模式,配置 AP 产品型号 AP220-SE、AP220-E 的系列名称为“RG-AP220”。
Ruijie (config)# ac-controller
Ruijie (config-ac)# ap-serial RG-AP220 AP220-SE AP220-E
!配置 RG-AP220 系列使用 ap.bin 文件升级。
Ruijie (config-ac)# ap-iamge RG-AP220 ap.bin
!激活 ap.bin 文件.
Ruijie (config-ac)# active-bin-file ap.bin
```

(4) 配置 AC 网络中的无线用户黑名单。

```
!在 AC 配置模式下,配置禁止 MAC 地址为 aaaa.bbbb.cccc 的无线用户上网。
Ruijie (config)# ac-controller
Ruijie (config-ac)# mac-acl aaaa.bbbb.cccc
```

(5) 配置指定 AP 的用户名和密码。

```
!配置 AP0001 的用户名为 Switch,密码为 123。
Ruijie (config)# ap-config AP0001
Ruijie (config-ap)# credential Switch 123
```

5.7 本章小结

本章介绍了常用网络设备的管理技术和方法。首先介绍了 Web、FTP、E-mail 等常用服务器的配置技术和管理方法;然后介绍了交换机、路由器等设备的管理;最后对网络隔离设备、电源、WLAN 等管理进行了简单介绍。

本章重点是理解常用网络设备的作用和功能,掌握常用网络设备的配置技术和管理方法。

习 题 5

一、选择题

1. 下列命令在连接到外部网络的接口上启用 NAT 的是(　　)。
   A. ip nat inside　　B. ip nat outside source
   C. ip nat outside　　D. set ip nat outside
2. 下列选项中是标准的 IP 访问列表的是(　　)。
   A. access-list 110 permit host 1.1.1.1
   B. access-list 1 deny 192.168.215.48 0.0.0.0
   C. access-list 1 permit 192.168.215.48 255.255.255.0
   D. access-list standard 1.1.1.1

3. 交换机如何知道将帧转发到哪个端口？(　　)。

A. 读取 ARP 地址　　B. 用 ARP 地址表

C. 读取源 MAC 地址　　D. 用 MAC 地址表

4. IEEE 制定了什么标准,规范了跨交换机实现 VLAN 的方法(　　)。

A. 802.1q　　B. ISL　　C. VTP　　D. 802.1x

二、简答题

1. 什么是虚拟主机？什么是虚拟目录？
2. 什么是物理隔离和逻辑隔离？
3. 简述跨交换机划分 VLAN 的方法。
4. 简述基于山特技术的 UPS 管理方案。
5. 接入服务器的功能是什么？
6. ACL 和 NAT 的作用是什么？

第6章 日常运维与管理

6.1 网站设计与管理

6.1.1 企业网站概述

1. 企业网站及其特征

网站的种类很多，如政府网站、教学网站、新闻媒体网站、供求信息发布网站、个人网站等。从网络技术的基本原理来看，各种网站并没有本质上的差别，不同之处主要在于网站的目的、内容、功能、规模、表现形式、经营方式等。

由于企业网站具有自主性和灵活性的特点，所以不同的企业网站之间不仅表现形式各有特色，功能和内容也千差万别。可以按照行业、企业规模、网站所采用的技术、网站主机类型等对其进行分类，如果从功能上考虑，可以将企业网站分为信息发布型和网上销售型两类。无论是哪种形式，通常企业网站一般具有如下一个或多个特征：

- 通过网站的形式向公众传递企业品牌形象、企业文化等基本信息。
- 发布企业新闻、供求信息、人才招聘信息。
- 向供应商、分销商、合作伙伴、直接用户等提供某种信息和服务。
- 网上展示、推广、销售商品。
- 收集市场信息、注册用户信息。
- 其他具有营销目的或营销效果的内容和形式。

因此，从营销的策略来看，企业网站是一个开展网络营销的综合性工具。

2. 企业网站的功能

(1) 品牌形象：网站的形象代表着企业的网上品牌形象，人们在网上了解一个企业的主要方式就是访问该企业的网站，网站建设的专业化与否直接影响企业的网络品牌形象，同时也对网站的其他功能产生直接影响。

(2) 产品/服务展示：顾客访问网站的主要目的是为了对企业的产品和服务进行深入的了解，企业网站的主要价值也就在于灵活地向用户展示产品说明及图片，甚至多媒体信息。即使一个功能简单的网站，至少也相当于一本可以随时更新的产品宣传资料。

(3) 信息发布：网站是一个信息载体，在法律许可的范围内，可以发布一切有利于企业形象、顾客服务以及促进销售的企业新闻、产品信息、各种促销信息、招标信息、合作信息、人员招聘信息等。因此，拥有一个网站就相当于拥有一个强有力的宣传工具。

(4) 顾客服务：通过网站可以为顾客提供各种在线服务和帮助信息，比如常见问题解

答(FAQ),在线填写寻求帮助的表单,通过聊天实时回答顾客的咨询等。

(5) 顾客关系:通过网络社区等方式吸引顾客参与,不仅可以开展顾客服务,同时也有助于增进顾客关系。

(6) 网上调查:通过网站上的在线调查表,可以获得用户的反馈信息,用于产品调查、消费者行为调查、品牌形象调查等,是获得第一手市场资料的有效调查工具。

(7) 网上联盟:为了获得更好的网上推广效果,需要与供应商、经销商、客户网站以及其他内容互补或者相关的企业建立合作关系,没有网站,合作就无从谈起。

(8) 网上销售:建立网站及开展网络营销活动的目的之一是为了增加销售,一个功能完善的网站本身就可以完成订单确认、网上支付等电子商务功能,即网站本身就是一个销售渠道。

3. 企业网站的要素

企业网站是一个可以发布企业信息、提供顾客服务,以及在线销售的渠道;而在开发设计人员看来,企业网站无非是一些功能模块,通过网页的形式将前台和后台结合起来。一个完整的企业网站,无论多么复杂或多么简单,都可以划分为网站结构、网站内容、网站服务和网站功能 4 个组成部分,这 4 个部分也就是组成企业网站的一般要素。

(1) 网站结构:为了向用户表达企业信息所采用的网站栏目设置、网页布局、网站导航、网址(URL)层次结构等信息的表现形式等。

(2) 网站内容:是用户通过企业网站可以看到的所有信息,也就是企业希望通过网站向用户传递的所有信息。网站内容包括所有可以在网上被用户通过视觉或听觉感知的信息,如文字、图片、视频、音频等。一般来说,文字信息是企业网站的主要表现形式。

(3) 网站功能:是为了实现发布各种信息,提供服务等必需的技术支持系统。网站功能直接关系到可以采用的网络营销方法以及网络营销的效果。

(4) 网站服务:即网站可以提供给用户的服务,如问题解答、优惠信息、资料下载等。网站服务是通过网站功能和内容而实现的。

6.1.2 基于网络营销的企业网站建设

1. 企业网站建设存在的问题

《大型企业网站营销状况研究报告》通过对国内 11 个行业的 117 家大型消费类企业网站所进行的系统调查发现,大型企业网站普遍存在的 10 个问题是:

(1) 总体策划目的不明确,缺乏网络营销思想指导。

(2) 栏目规划不合理,导航系统不完善。

(3) 信息量小,重要信息不完整。

(4) 促销意识不够明确。

(5) 服务尤其是在线顾客服务比较欠缺。

(6) 对销售和售后服务的支持作用未得到合理发挥。

(7) 在网络营销资源积累方面缺乏基本支持。

(8) 过于追求美术效果,美观有余而实用不足,甚至影响正常浏览和应用。

(9) 优化设计的基本思想和内容没有得到起码的体现。

(10) 访问量小,急需有效的网站推广策略。

企业网站之所以存在这些问题，主要原因在于对企业网站本质的认识不够，网站建设的全局意识差，以及企业对网络营销价值和策略没有足够的重视等。因此企业网站的建设需要引起足够的重视，需要在网站的易用性、可信度、网站优化等方面进行认真研究，并学会对网站的评价和诊断技术。

2. 企业网站的易用性

企业网站应该具有易用性，网站易用性的核心思想是网站设计以用户为导向，通过最简单、醒目、易用的网站要素设计、清晰的字体和链接、网页标题和内容的可读性、网页设计对搜索引擎友好、网页设计对浏览器兼容性、合理利用音频视频等多媒体文件、多语言版本以及适应不同用户群体的浏览等。美国咨询公司 Nielsen Norman Group 调查发现，影响易用性的主要问题有：

(1) 网站设计差。

(2) 内容贫乏。

(3) 产品介绍不完整令潜在客户产生疑虑和不信任。

(4) 糟糕的导航结构让潜在客户失去耐心等。

3. 企业网站的可信度

网站的可信度就是用户对网站的信任程度，其对网络营销具有重要的现实意义。据调查，影响网站可信度的问题包括如下内容：

(1) 网站基本信息不完整。如不谈企业的产品、实力和信誉等问题。

(2) 产品介绍过于简略，客户无法判断产品的价值。

(3) 没有明确的个人信息保护声明，用户注册时填写信息过于详细。

(4) 没有固定联系方式。

(5) 使用免费邮箱。

(6) 网站信息久不更新。

(7) 网站计数器显示访问者数量少。

(8) 付款方式的影响。如收款人是个人储蓄账户等。

在基于网络营销企业网站的建设中需要认真对待这些细节。

4. 企业网站的优化

为了突出企业网站网络营销的效果，应该注意网站的优化，即通过对网站功能、网站结构、网页布局和内容等关键要素的合理设计，使得网站的功能和表现形式达到最优效果，可以充分表现出网站优化的期望结果。网站优化的含义包括对用户优化、对网络环境(包括搜索引擎等)优化、对网站维护优化 3 个层面。网站优化的设计应该遵循下面的原则：

(1) 坚持用户导向而不是搜索引擎导向。

(2) 网站优化的基础是网站的结构、内容、功能和服务。

6.1.3 企业网站的管理

网站管理的目的是为了让企业网站能够长期安全、稳定地运行，及时地调整和更新网站内容，以便在瞬息万变的信息海洋中抓住更多的商机。网站管理是一项专业性较强的工作，其管理的内容也非常丰富，包括服务器及相关软硬件的维护、数据库维护、功能改进、页面修改、信息发布、网站推广、网站优化、网络数据分析、安全管理等内容。

本节以 SiteFactory 专业版为例来说明企业网站的后台管理操作，读者可以登录 http://demo.powereasy.net 网站体验。SiteFactory 的后台管理功能主要包括我的工作台、信息管理、内容相关、问答管理、用户管理、附件管理和系统设置等模块，其主页如图 6-1 所示。



图 6-1　SiteFactory 专业版后台管理主页面

1. 我的工作台

(1) 工作台首页：不同管理员拥有独立的管理界面，可以自由对信息、日历、待签文章、短消息、备忘录等进行参数设置、布局排版、添加删除。添加模块的操作如图 6-2 所示，在“我的工作台”首页中，用鼠标左键单击“内容信息”下拉列表框，选择需要添加的模块，接着选择其所放的位置：“左边”或“右边”，然后单击“添加模块”按钮即可。



图 6-2　添加管理模块页面

(2) 主题控制：不同管理员可以单独设置后台管理的界面风格，系统内置了 3 套界面风格供选择。

(3) 快捷导航配置：在左侧的“快捷导航”栏中，系统提供了管理项目的拖曳排序功能。用鼠标左键单击管理项目名后上下拖动，放置到合适序位后再松开鼠标左键即可。预设好

管理项目后,管理员每次进入管理后台都可以单击其项目快速管理相关信息。由于采用了AJAX技术,以上导航配置操作将实时保存。

(4) 我的权限:能够显示登录管理员的后台操作权限,方便进行管理员管理及权限调整等。

(5) 修改密码:提供管理员登录账号的密码修改和重置功能。

(6) 使用帮助:提供后台使用时的帮助信息及FAQ等信息。

(7) 切换管理员身份:方便超级管理员对下属管理员进行快捷操作管理,可以在不退出的情况下进入到指定管理员后台进行各种管理操作。

(8) 安全退出:提供管理员退出管理后台的快捷途径,避免账号异常丢失。

2. 信息管理

(1) 内容管理:如图6-3所示,信息管理提供对网站所有信息进行添加、删除、查询、搜索、签收、审核、归档、替换、退稿等丰富的信息管理功能,可按照栏目和专题两种方式对信息进行管理,以方便构建强大的内容信息管理与交互平台。



图6-3 内容管理页面

(2) 自定义表单管理:提供自定义提交内容的在线表单系统,通过自定义表单系统可以方便地构建各种在线提交表单,如报名表、调查表、预订表等。同时,能够在后台查看每个表单的提交数据,并进行管理。

(3) 专题内容管理:提供快速构建各种内容专题的功能,可以将网站所有信息有选择地调用到不同专题下,且专题支持自定义模板和链接后缀。方便用户构建形式各样的内容专题。

(4) 节点搜索:提供对后台所有节点的快速搜索功能,可直接输入节点名称进行便捷搜索和查找。

(5) 图片在线剪切:提供了对文章首页图片进行在线自由裁剪的功能,可根据首页图片尺寸来自行裁剪,而无须在其他工具中处理好才上传,大大减轻了管理员的工作量,提高了工作效率。

(6) 回收站管理:网站所有删除的信息都进入到回收站进行保存,并可以根据节点来进行查询和浏览。回收站的所有信息都提供了彻底删除与恢复功能,帮助用户更有效地对信息内容进行管理。

(7) 生成HTML管理:提供网站静态页面的生成管理功能。管理员可以根据内容页、栏目页、单独页面、专题页面的分类依次生成;可以按照时间、生成页面数量、信息ID号区

间等分类来生成；也可以定时、定量对信息进行生成。

(8) 签收管理：提供特殊信息的签收功能，可以按照所有文档、公众文档、专属文档、签收中的文档4种分类进行签收文档查看；保障信息的保密性、时效性和监督性。

(9) 归档内容：系统提供对不想显示在前台但需要保留的这一类信息进行存放的功能，用户可以通过归档功能将这类信息进行归档，以便日后进行搜索和再利用。

(10) 批量替换：提供根据栏目、模型、模型中字段3种条件进行内容的批量替换。批量替换功能方便用户对信息进行批量处理，特别是对采集回来的文章、含有错误内容的信息进行替换操作，提升信息管理的效率。

(11) 高级查询：提供根据所属节点、所属模型、所属模型中字段3种条件对网站所有信息进行筛选查询，方便用户对特定的批量信息进行搜索和管理，有利于提升信息管理的效率。

3. 内容相关

(1) 生成管理：生成管理包括生成内容页、生成单页节点、生成栏目页、生成专题类别页、生成专题列表页、生成网站综合数据等功能。其中，生成内容页提供根据最新N个项目进行生成，根据时间段进行生成，根据信息ID段进行生成，根据指定信息ID号进行生成，根据生成未生成信息等多种条件的内容页生成方式，操作页面如图6-4所示。



图 6-4　生成内容页面

(2) 采集项目管理：如图6-5所示，采集项目管理模块可以直接深入指定站内或者页面中，根据不同规则将网页中的有效数据采集出来（而不仅是网页或链接），保持数据之间逻辑关系之后，将数据录入进网站数据库中。以维护一个新闻站点为例，采集管理可以将每个新闻的标题、正文等信息单独采集出来，分别作为字段存储在系统中。在提高信息录入效率的同时，也最大限度地减轻用户工作的负担。

(3) 评论管理：提供强大的AJAX.NET无刷新评论功能，不同用户可以针对某一篇信息发表评论，同时可以对评论观点进行多人的辩论PK，管理员在后台可以对评论进行审核、修改、回复、删除等操作。



图 6-5　采集项目管理页面

(4) 工作量统计：为方便统计网站中的相关信息，管理员可以按栏目/月份，按栏目/录入者，按栏目/审核者，按录入者/月份，按审核者/月份统计网站相关信息。

(5) 站内链接管理：站内链接是对网站内所有信息中指定内容自动添加指定链接目标的功能，例如，添加一个名为“动易”的站内链接，网站文章中如果有“动易”字样时，系统自动给“动易”这个词加上链接地址，以链接到一个特定的页面中。

(6) 关键字过滤：网站是一个互动的信息交流平台，会员可以发布信息、发表评论等以增强网站的交互性。但有时会员发布的信息中会出现一些不想要的信息，这时可以利用系统提供的关键字过滤功能，自动过滤相关的信息。

(7) 其他管理：方便管理员对网站某些信息的管理，如关键字管理、作者管理、来源管理、下载服务器管理、下载报错管理等功能。

4. 问答管理

问答管理提供对问答平台所有问题和回答的统一管理，能够有效地提高管理员对平台中信息内容的把握和管理能力。

(1) 头衔系列管理：提供根据不同积分设置不同头衔的功能，且能够添加多种不同的头衔系列。通过头衔系列功能能够有效地提升前台会员的参与热情，增加问答平台与网友的粘性。

(2) 问答积分明细管理：提供问答平台所有积分明细查看功能，方便管理员掌握积分发放情况，有效组织各种有奖活动和人员奖励等，增强整个问答平台的 Web 2.0 特性。

5. 用户管理

(1) 管理员管理：管理员是指网站中拥有相应网站管理权限的特殊会员，每个管理员都有其相应的管理角色，同时与前台一个注册会员相对应。管理员管理可以设置不同的后台管理权限。

(2) 角色管理：角色是用户在某个环境中的身份，这个身份拥有某些与其行为相匹配的权限，包括网站管理权限。如果修改了角色所拥有的权限，其相应的管理员权限也将随之变化。角色也是一种自定义权限的集合，在添加管理员的时候可以赋予管理员不同的角色，也允许预设多个角色，并可以为每个角色指定相关管理权限。

(3) 会员管理：会员是在本站注册的用户。管理员可以单独对某个会员设置不同的权限并进行管理，也可以利用会员组功能以批量设置从属于同一会员组中的会员权限。添加新会员的页面如图 6-6 所示。



图 6-6 添加新会员页面

(4) 推广管理：可对会员注册推广进行各种管理，包括填写个人推广会员信息、查看推广项目、查询个人推广情况等操作。

(5) 充值卡管理：网站中可以发行真实的充值卡，会员直接购买后可以输入卡号和密码进行充值（为了安全，数据库中保存的充值卡密码都是经过加密的）。也可以通过网站销售虚拟的充值卡，会员在购买虚拟充值卡后，在线获得充值卡号和密码，并进行充值。充值卡充值的所有操作都有明细记录以供查询。网站充值卡功能支持点数卡、天数卡、月卡、年卡等类型。添加充值卡页面如图 6-7 所示。



图 6-7 添加充值卡页面

(6) 资金明细：本功能用于记录、查询和显示网站中所有资金明细、在线支付明细、会员点券明细、会员有效期明细等明细记录，以方便管理员分析会员消费习惯、查询资金交易记录。

(7) 会员点券明细：本功能用于记录、查询和显示网站中所有会员的点券消费情况、收支情况等明细记录，以方便管理员分析会员消费习惯、查询资金交易记录。

(8) 会员有效期明细：本功能用于记录、查询和显示网站中所有会员的有效期情况、添加扣除情况等明细记录。

(9) 在线支付明细：本功能用于记录、查询和显示网站中所有在线支付情况、支付成功/未成功情况等明细记录，以方便管理员掌握网站资金往来情况、查询资金交易记录。

6. 附件管理

(1) 广告管理：广告管理中包含了广告版位管理和广告管理功能。广告版位是指预设了矩形、横幅、弹出窗口、随屏移动、漂浮移动等类型、尺寸、显示方式的广告类型集合，它以JS代码的方式在前台进行调用。同一广告版位可以包含多个广告，同一广告也可以从属于不同的广告版位，并可设置广告权重及显示方式来显示广告。添加新广告页面如图 6-8 所示。



图 6-8 添加新广告页面

(2) 问卷调查管理：本功能提供了较为丰富的表达定制功能，使用内置的功能项能够轻松地制作并实现各种问卷调查、市场调查、报名表制作、酒店预订等功能。

(3) 网站访问统计：本功能可以方便站长分析网站的运营情况；可以查看访问统计分析、访问统计参数配置、统计 IP 库添加、统计 IP 库管理、统计代码调用和统计数据初始化等功能分类。系统准确统计网站的在线用户的详情，如 IP、上站时间、停留时间和所在页面及客户端信息等，统计报告如图 6-9 所示。

(4) 信息发送管理：会员在网站前台会员中心功能中，可以利用系统提供的短消息功



图 6-9　网站统计报告页面

能向其他单个或多个会员发送站内短消息。系统后台提供了短消息管理功能，管理员既可以在管理会员间发送站内短消息，也可以在后台向指定的会员或会员组单发或群发短消息（前台会员可以在会员中心的短消息管理中查阅到短消息）。短消息管理页面如图 6-10 所示。

图 6-10　短消息管理页面

(5) 邮件列表管理：系统提供向本站注册用户所填写的邮件地址批量发送邮件的功能，管理员可以在后台向指定的会员或会员组单发或群发邮件。邮件发送页面如图 6-11 所示。



图 6-11　邮件发送页面

(6) 网站日志管理：系统提供站内日志功能，对管理员登录、日常操作、越权操作、黑客攻击等都将以日志方式进行记录，方便超级管理员进行查询。超级管理员可以删除和清空两天前的日志(两天内的日志即使是超级管理员也不能删除)。超级管理员可以随时通过日志分析发现问题出现的原因。

(7) 在线比较文件：在线比较网站文件功能是在线比较 Web 空间中的网站可运行文件和动易官方发布的相应版本中原始可运行文件，方便管理员对比和管理 Web 空间文件。

(8) 上传文件管理：在添加信息时经常要上传图片等文件，系统提供了上传文件管理功能，以方便用户管理所上传的图片、Word 文档、压缩包等文件。对于图片类型的文件，可以进行鼠标预览或以缩略图方式预览。同时，在服务器空间有限时，可以删除不再使用的文件，以节省空间。上传文件管理页面如图 6-12 所示。

(9) 缓存管理：为了加快访问速度，系统全面引入服务器端缓存技术。缓存可以先把数据预写到服务器的缓存中，需要时直接从缓存中读出而无须在数据库中进行数据库查询，这就缩短了 CPU 的运算时间以减少服务器端压力，加快客户端的浏览速度。

7. 系统设置

(1) 网站配置：提供网站基本信息的快速配置功能，如网站的名称、标题、网站地址、Logo 与 Banner 地址、站长姓名与信箱、版权、网站 Meta 关键词与网页描述、缩略图设置、WAP/RSS 功能设置、手机短信、IP 限制设置、用户参数设置等基本信息。

(2) 内容模型管理：内容模型是网站内某类功能管理的集合体。根据栏目需要预先设置好相应字段及其属性以适用于不同的用途，所有模型的所有字段都可以由企业用户进行控制。内容模型可以根据不同的应用需求快捷有效地设置和管理不同类型、不同属性的信



图 6-12　上传文件管理页面

息，如“文章”、“下载”、“图片”、“内容”、“公告”、“友情链接”、“留言”、“供求信息”、“房产信息”等功能模块。

(3) 节点管理：节点是为了对信息进行分类管理而设定的分类方式；可以设置不同的管理权限和访问权限，同时可以指定不同的模板；可以分为栏目节点、单页节点、外部链接等多个类型。节点是传统网站栏目和频道的高级应用，可以更高效、合理地构建网站栏目和管理网站栏目。

(4) 专题管理：将分布在不同栏目的信息按某一主题进行分类和汇总，如某些信息虽分布在不同的栏目，但同属于一个主题，这时就可以建立专题进行管理，从而为网站的信息分类提供极大的灵活度。专题类别的添加页面如图 6-13 所示。

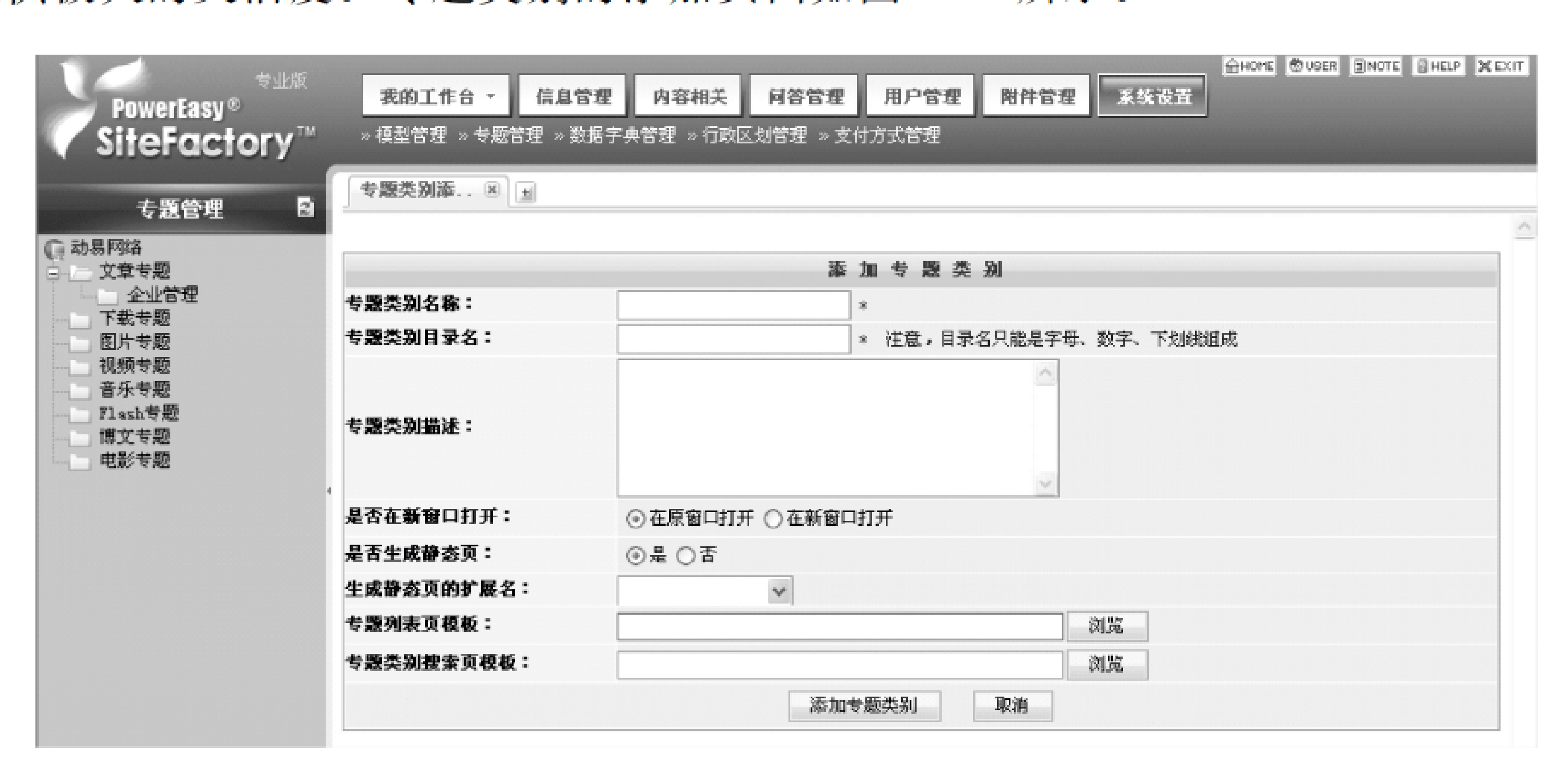


图 6-13　专题类别添加页面

(5) 模板标签管理：独创的“Xpower 模板引擎”模式，吸取了 XML、XSLT 等技术的优点，将 VS2005 中的很多概念重构为可在线使用的版本，引入了如“数据源”、“字段格式处理”、“内容标签”、“循环标签”、“自由分页”等方法，成功实现了完全跨页面的标签调用方式和标签无限级嵌套等功能。软件使用者借助“网站模板与网站程序完全分离”和“模板方案”的全新概念，让网站的模板设计与程序彻底分开。可以为每个频道、栏目甚至内容页面设置不同的模板，随时编辑、修改网站界面，更能够一键切换预设的模板方案，瞬间更换网站界面。

(6) 数据字典管理：由于企业在不同行业、不同领域都有自己的客户群体，其关系信息有着很大的区别。为此系统提供了灵活便捷的“数据字典”功能，根据企业的实际客户定位与需要，合理设置如客户区域/所属行业/价值评估等各项参数，对系统提供的客户关系管理中相关信息进行个性化设置，方便企业实现以客户为中心的管理思想，始终专注于客户生命周期价值，为企业发展带来更强的竞争能力。

(7) 行政区划管理：行政区划是国家对地方行政区域、行政建制的划分与设置，如省、市、州、县、乡、镇等。系统提供了行政区划管理和预设功能，预设好相关行政区划后，在网站后台设置(如“所在的地区”)，前台客户订购流程中“收银台”的收货人地址等操作中可以快捷地选择所属的行政区划。

(8) 银行账户管理：在银行账户中可以添加和设置网站中所使用的银行账户，以方便客户在选购商品并提交订单后能查阅与选择相应的银行账户进行付款。银行账户可用于会员资金管理与消费管理中各种收费管理操作，同时也用于按银行名查询资金明细记录。添加银行账户页面如图 6-14 所示。



图 6-14　添加银行账户页面

(9) 在线支付平台管理：系统内置了 13 种在线支付平台接口，软件用户只需输入相应的密钥和信息就可以使用了。这些平台包括财付通、支付宝、快钱、上海环讯、网银在线、云网支付、易付通等。添加在线支付平台页面如图 6-15 所示。



图 6-15　添加在线支付平台页面

6.2 网络布线管理

6.2.1 网络综合布线系统

1. 网络综合布线系统的基本概念

网络综合布线系统(以下简称“综合布线系统”)是一套用于建筑物内或建筑群之间为计算机、通信设施与监控系统预先设置的信息传输通道。它将语音、数据、图像等设备彼此相连,同时能使上述设备与外部通信数据网络相连接。综合布线系统为智能大厦和智能建筑群中的信息设施提供了多厂家产品兼容,模块化扩展、更新与系统灵活重组的可能性。既为用户创造了现代信息系统环境,强化了控制与管理,又为用户节约了费用,保护了投资。综合布线系统已成为现代化建筑的重要组成部分。

2. 综合布线系统的特点

采用星型拓扑结构、模块化设计的综合布线系统,与传统的布线相比具有开放性、灵活性、模块化、扩展性及独立性等特点。

(1) 开放性:综合布线系统采用开放式体系结构,符合国际标准,它几乎对所有厂商的产品都是开放的。使得设备的更换或网络结构的变化都不会导致综合布线系统的重新铺设,只需进行简单的跳线管理即可。

(2) 灵活性:综合布线系统采用星型结构,可以在综合布线系统管理间进行灵活的跳线管理,使系统变化成星型、环型、总线型等不同的逻辑结构,实现不同拓扑结构的组网需求;当终端设备位置需要改变时,除了进行跳线管理外,不需要进行更多的布线改变;同时,综合布线系统还能够满足多种应用的要求,能够灵活地连接不同类型的应用设备。

(3) 模块化:综合布线系统的接插元件,如配线架、终端模块等采用积木式结构,可以方便地进行更换插拔,使管理、扩展和使用变得十分简单。

(4) 扩展性:综合布线系统严格遵循国际标准,因此,无论计算机设备、通信设备、控制设备随技术如何发展,将来都可很方便地将这些设备连接到系统中去。综合布线系统灵活的配置为应用的扩展提供了较高的裕量。系统采用光纤和双绞线作为传输介质,为不同应用提供了合理的选择空间。

(5) 独立性:综合布线系统的最根本的特点是独立性。采用综合布线方式进行物理布线时,不必过多地考虑网络的逻辑结构,更不需要考虑网络服务和网络管理软件,也就是说,综合布线系统与应用具有独立性。

3. 综合布线系统的组成

如图 6-16 所示,综合布线系统由工作区子系统、水平区子系统、管理间子系统、垂直干线子系统、设备间子系统及建筑群子系统 6 个子系统组成。由于采用星型结构,任何一个子系统都可独立地接入综合布线系统中。因此,系统易于扩充,布线易于重新组合,也便于查找和排除故障。

(1) 工作区子系统

工作区子系统是一个可以独立设置终端设备的区域,该子系统包括水平配线系统的信息插座、连接信息插座和终端设备的跳线以及适配器。工作区的服务面积一般可按 5～

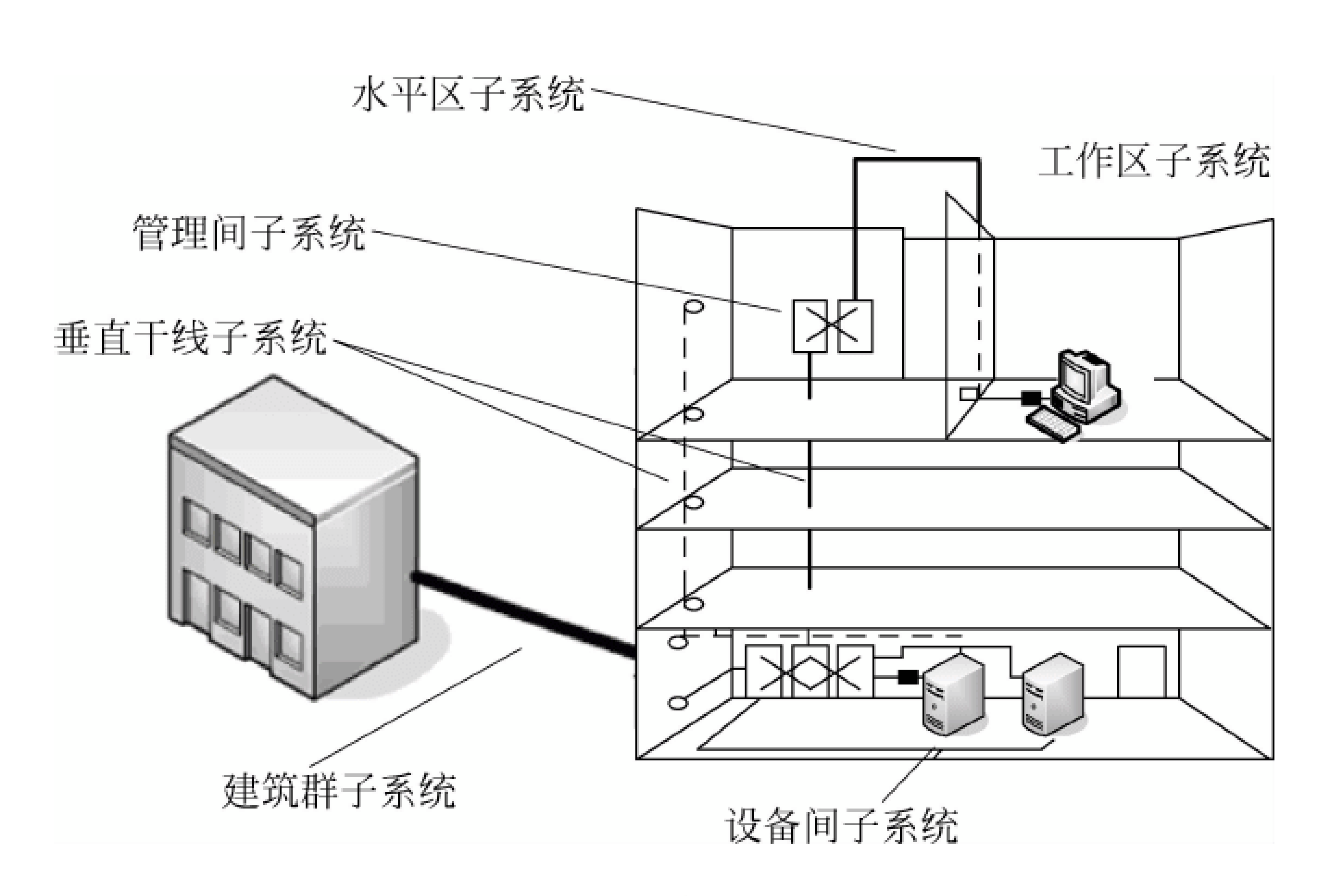


图 6-16　综合布线系统

$10m^2$ 估算，工作区内信息点的数量根据相应的设计等级要求设置。工作区的每个信息插座都应该支持电话机、数据终端、计算机及监视器等终端设备。

(2) 水平区子系统

水平区子系统应由工作区用的信息插座、楼层分配线设备至信息插座的水平电缆、楼层配线设备和跳线等组成。一般情况下，水平电缆应采用 4 对双绞线电缆。在水平区子系统中有高速率应用的场合，应采用光缆，即光纤到桌面。水平区子系统根据整个综合布线系统的要求，应在二级交接间、交接间或设备间的配线设备上进行连接，以构成电话、数据、电视系统和监视系统，并方便地进行管理。水平区子系统的电缆长度应小于 90m，信息插座应在内部做固定线连接。

(3) 管理间子系统

管理间子系统设置在楼层分配线设备的房间内。管理间子系统应由交接间的配线设备、输入输出设备等组成，也可应用于设备间子系统中。管理间子系统应采用单点管理双交接，交接场的结构取决于工作区、综合布线系统的规模和选用的硬件。在管理规模大、复杂度高、有二级交接间时才设置双点管理双交接。在管理点，应根据应用环境用标记插入条来标出各个端接场。交接区应有良好的标记系统，如建筑物名称、建筑物位置、区号、起始点和功能等标志。交接间和二级交接间的配线设备应采用色标区别各类用途的配线区。

(4) 垂直干线子系统

垂直干线子系统应由设备间的配线设备和跳线，以及设备间至各楼层分配线间的连接电缆组成。在确定垂直子系统所需要的电缆总对数之前，必须确定电缆中语音和数据信号的共享原则。对于基本型，每个工作区可选定 2 对双绞线；对于增强型，每个工作区可选定 3 对双绞线；对于综合型，每个工作区可在基本型或增强型的基础上增设光缆系统。

如果设备间与计算机机房处于不同的地点，而且需要把语音电缆连至设备间，把数据电缆连至计算机机房，则应在设计中选取不同的干线电缆或干线电缆的不同部分来分别满足不同路由的语音和数据需要。当必要时，也可以采用光缆系统予以满足。

(5) 设备间子系统

设备间是在每一幢大楼的适当地点设置进线设备，进行网络管理以及管理人员值班的

场所。设备间子系统应由综合布线系统的建筑物进线设备、电话、数据、计算机等各种主机设备及其保安配线设备等组成。设备间内的所有进线终端设备应采用色标区别各类用途的配线区。设备间位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。

(6) 建筑群子系统

建筑群子系统由2个以上建筑物的电话、数据、监视系统组成的建筑群综合布线系统，其连接各建筑物之间的缆线和配线设备，组成建筑群子系统。建筑群子系统应采用地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各项设计规定。此外，安装时至少应予留1～2个备用管孔，以供扩充之用。建筑群子系统采用直埋沟内敷设时，如果在同一个沟内埋入了其他的图像、监控电缆，应设立明显的共用标志。

6.2.2 网络综合布线工程设计

1. 工作区子系统设计

工作区子系统由终端设备和连接到信息插座的跳线组成，它包括信息插座、信息模块、网卡和连接所需的跳线，并在终端设备和输入输出之间搭接，相当于电话配线系统中连接话机的用户线及话机终端部分。终端设备可以是电话、PC和数据终端，也可以是绘图仪、打印机或扫描仪。

(1) 设计要点

- 工作区内线槽要布局合理、美观。
- 信息插座要设计在距离地面30cm以上。
- 信息插座与计算机设备的距离保持在5m范围内。
- 购买的网卡类型接口要与线缆类型接口保持一致。
- 确定所有工作区所需的信息模块、信息插座、面板的数量。
- 确定RJ-45接头所需的数量。

(2) 所需配件的计算

- RJ-45接头的需求量一般用下述公式计算：

$$m=n\times4+n\times4\times15\%$$

  其中，m为RJ-45总需求量；n为信息点的数量；$n\times4\times15\%$为留有的富余量。

- 信息模块的需求量一般用下述公式计算：

$$m=n+n\times3\%$$

  其中，m为信息模块的总需求量；n为信息点的总量；$n\times3\%$为留有的富余量。

- 每个工作区至少要配置一个插座盒。对于难以再增加插座盒的工作区，要至少安装两个分离的插座盒。

2. 水平区子系统设计

水平区子系统是从工作区的信息插座开始到管理间子系统的配线架，设计涉及水平区子系统的传输介质和部件集成。

水平布线可选择的介质有3种(100Ω的UTP电缆、150Ω的STP电缆及62.5/125μm光缆)，最远的延伸距离为90m，除了90m水平电缆外，工作区与管理子系统的接插线和跨接线电缆的总长可达10m。一般情况下，水平电缆应采用4对双绞线电缆。在水平区子系统有高速率应用的场合，应采用光缆，即光纤到桌面。水平区子系统根据整个综合布线系统

的要求，应在二级交接间、交接间或设备间的配线设备上进行连接，以构成电话、数据、电视系统和监视系统，并方便地进行管理。

(1) 设计要点

- 根据工程提出近期和远期的终端设备要求。
- 每层需要安装的信息插座数量及其位置。
- 终端将来可能产生移动、修改和重新安排的详细情况。
- 一次性建设与分期建设的方案比较。
- 确定线路走向。
- 线缆、槽、管的数量和类型。
- 采用吊杆还是托架方式走线槽。
- 语音点、数据点互换时，要注意语音水平线缆与数据线缆的类型。

确定线路走向一般要由用户、设计人员、施工人员到现场根据建筑物的物理位置和施工难易度来确立。信息插座的数量和类型、电缆的类型和长度一般在总体设计时便已确立，但考虑到产品质量和施工人员的误操作等因素，在订购时要留有余地。

在水平布线通道内，关于电信电缆与分支电源电缆需说明以下几点：

- 屏蔽的电源导体(电缆)与电信电缆并线时不需要分隔。
- 可以用电源管道障碍(金属或非金属)来分隔电信电缆与电源电缆。
- 对非屏蔽的电源电缆，最小距离为 0.1m。
- 在工作站的信息口或间隔点，电信电缆与电源电缆的距离最小应为 0.06m。

水平间设计的最后一点是确定水平间与干线接合配线管理设备。打吊杆走线槽时，一般是间距 1m 左右设置一对吊杆。吊杆的总量应为水平干线的长度(m)×2(根)。使用托架走线槽时，一般是 1～1.5m 安装一个托架，托架的需求量应根据水平干线的实际长度计算。托架应根据线槽走向的实际情况来选定。

水平布线是将电缆线从管理间子系统的配线间接到每一楼层的工作区的信息输入输出插座上。设计时要根据建筑物的结构特点，从路由(线)最短、造价最低、施工方便、布线规范等几个方面考虑。由于建筑物中的管线比较多，往往要遇到一些矛盾，所以，设计水平区子系统时必须折中考虑，择优选择最佳的水平布线方案。一般可采用以下 3 种方式：直接埋管式；先走吊顶内线槽，再走支管到信息出口的方式；适合大开间及后打隔断的地面线槽方式。

(2) 计算电缆公式

- 订货总量(总长度 m)＝所需总长＋所需总长×10%＋n×6

  其中，所需总长指 n 条布线电缆所需的理论长度；所需总长×10%为备用部分；n×6 为端接容差。
- 整幢楼的用线量＝$\sum NC$

  其中，N 为楼层数；C 为每层楼用线量，且 $C=[0.55\times(L+S)+6]\times n$

  该式中的 L 为本楼层离水平间最远的信息点距离；S 为本楼层离水平间最近的信息点距离；n 为本楼层的信息插座总数。
- 用线总长度＝$A+B/2\times n\times 3.3\times 1.2$

其中，A 为最短信息点长度；B 为最长信息点长度；n 为楼内需要安装的信息点数；系

数 3.3 的意义为将米换算成英尺；1.2 为余量参数(富余量)。

- 用线箱数＝总长度/1000＋1

3. 垂直干线子系统设计

垂直干线子系统的任务是通过建筑物内部的传输电缆，把各个服务接线间的信号传送到设备间，直到传送到最终接口，再通往外部网络。它必须满足当前的需要，又要适应今后的发展。垂直干线子系统的结构是一个星型结构。

垂直干线子系统包括供各条干线接线间之间的电缆走线用的竖向或横向通道，主设备间与计算机中心间的电缆两项。

1）设计要点

- 确定每层楼的干线要求。
- 确定整座楼的干线要求。
- 确定从楼层到设备间的干线电缆路由。
- 确定干线接线间的结合方法。
- 选定干线电缆的长度。

2）垂直干线子系统设计方法

确定从管理间到设备间的干线路由，应选择干线段最短、最安全和最经济的路由，在大楼内通常有如下两种方法。

(1) 电缆孔方法：干线通道中所用的电缆孔是很短的管道，通常用直径为 10cm 的钢性金属管做成。它们嵌在混凝土地板中，这是在浇注混凝土地板时嵌入的，比地板表面高出 2.5～10cm。电缆往往捆在钢绳上，而钢绳又固定到墙上已铆好的金属条上。当配线间上下都对齐时，一般采用电缆孔方法。

(2) 电缆井方法：电缆井方法常用于干线通道。电缆井是指在每层楼板上开出一些方孔，使电缆可以穿过这些方孔并从某层楼伸到相邻的楼层。电缆井的大小依所用电缆的数量而定。与电缆孔方法一样，电缆也是捆在或箍在支撑用的钢绳上，钢绳靠墙上金属条或地板三脚架固定住。离电缆井很近的墙上立式金属架可以支撑很多电缆。电缆井的选择性非常灵活，可以让粗细不同的各种电缆以任何组合方式通过。电缆井方法虽然比电缆孔方法灵活，但在原有建筑物中开电缆井安装电缆造价较高，它的另一个缺点是使用的电缆井很难防火。如果在安装过程中没有采取措施防止损坏楼板支撑件，则楼板的结构完整性将受到破坏。

在多层楼房中，经常需要使用干线电缆的横向通道才能从设备间连接到干线通道，以及在各个楼层上从二级交接间连接到任何一个配线间。

3）注意事项

(1) 光纤铺设注意事项

- 光纤电缆铺设时不应该绞结。
- 光纤电缆在室内布线时要走线槽。
- 光纤电缆在地下管道中穿过时要用 PVC 管。
- 光纤电缆需要拐弯时，其曲率半径不能小于 30cm。
- 光纤电缆的室外裸露部分要加铁管保护，铁管要固定牢固。
- 光线电缆不要拉得太紧或太松，要有一定的膨胀收缩余量。

- 光线电缆埋地时，要加铁管保护。

（2）双绞线铺设注意事项

- 双绞线铺设时线要平直，走线槽，不要扭曲。
- 双绞线的两端点要标号。
- 双绞线的室外部分要加套管，严禁搭接在树干上。
- 双绞线不要拐硬弯。

4. 管理间子系统设计

1）设计要点

管理间子系统的设计主要包括管理交接方案、管理连接硬件和管理标记。管理交接方案提供了交连设备与水平线缆、干线线缆连接的方式，从而使综合布线及其连接的应用系统设备、器件等构成一个有机的整体，并为线路调整管理提供了方便。

管理间子系统使用色标来区分配线设备的性质，标识按性质排列的接线模块，标明端接区域、物理位置、编号、容量、规格等，以便维护人员在现场一目了然地加以识别。综合布线使用3种标记：电缆标记、场标记和插入标记。电缆和光缆的两端应采用不易脱落和磨损的不干胶条标明相同的编号。

2）管理间子系统的管理标识编制的原则

（1）规模较大的综合布线系统应采用计算机进行标识管理，简单的综合布线系统应按图纸资料进行管理，并应做到记录准确、更新及时、便于查阅。

（2）综合布线系统的每条电缆、光缆、配线设备、端接点、安装通道和安装空间均应给定唯一的标志。标志中可包括名称、颜色、编号、字符串或其他组合。

（3）配线设备、线缆、信息插座等硬件均应设置不易脱落和磨损的标识，并应有详细的书面记录和图纸资料。

（4）电缆和光缆的两端均应标明相同的编号。

（5）设备间、交接间的配线设备宜采用统一的色标区别各类用途的配线区。

3）管理间子系统交接方案

管理间子系统的交接方案有单点管理和双点管理两种。交接方案的选择与综合布线系统规模有直接关系，一般来说，单点管理交接方案应用于综合布线系统规模较小的场合，而双点管理交接方案应用于综合布线系统规模较大的场合。

（1）单点管理交接方案

单点管理属于集中型管理，通常线路只在设备间进行跳线管理，其余地方不再进行跳线管理，线缆从设备间的线路管理区引出，直接连到工作区，或直接连至第二个接线交接区。

单点管理交接方案中管理器件放置于设备间内，由它来直接调度控制线路，实现对终端用户设备的变更调控。单点管理又可分为单点管理单交接和单点管理双交接两种方式。单点管理双交接方式中，第二个交接区可以放在楼层配线间或放在用户指定的墙壁上。

（2）双点管理交接方案

双点管理属于集中、分散型管理，除在设备间设置一个线路管理点外，在楼层配线间或二级交接间内还设置第二个线路管理点。这种交接方案比单点管理交接方案提供了更加灵活的线路管理功能，可以方便地对终端用户设备的变动进行线路调整。

一般在管理规模比较大，而且复杂又有二级交接间的场合，采用双点管理双交接方案。

如果建筑物的综合布线规模比较大，结构也较复杂，还可以采用双点管理 3 交接，甚至采用双点管理 4 交接方式。综合布线中使用的电缆，一般不能超过 4 次连接。

5. 设备间子系统设计

设备间是布线系统最主要的管理区域，所有楼层的信息都由电缆或光纤电缆传送至此。设备间子系统由设备室的电缆、连接器和相关支撑硬件组成，通过电缆把各种公用系统设备互连起来。它是一个公用设备存放的场所，也是设备日常管理的地方。

设备间内的所有进线终端设备应采用色标区别各类用途的配线区。设备间位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。设备间设计时，最低高度、房间大小、照明设施、地板负重、电气插座、配电中心、管道位置、楼内气温控制、门的方向与位置、端接空间、接地要求、备用电源、保护设施、消防设施等环境条件要素必须符合国家规定的标准。应尽量满足下面的要求：

- 设备间应设在位于干线综合体的中间位置。
- 应可能靠近建筑物电缆引入区和网络接口。
- 设备间应在服务电梯附近，便于装运笨重设备。
- 防止可能的水害（如暴雨、自来水管爆裂等）带来的灾害。
- 尽量远离有害气体源，避免腐蚀、易燃、易爆物和电磁场的干扰。
- 设备间空间（从地面到天花板）应保持 2.5～3.2m 高度的无障碍空间，门高≥2.1m，宽≥90m，地板承重压力不能低于 500kg/m^2。
- 室温应保持在 18～27℃之间，相对湿度保持在 30%～ 55%。
- 保持室内无尘或少尘，通风良好。
- 安装合适的消防系统（如采用湿型消防系统，不要把喷头直接对准电气设备）。
- 使用防火门，至少能耐火 1h 的防火墙和阻燃漆。
- 提供合适的门锁，至少要有一扇窗留作安全出口。
- 根据结构化布线系统的要求，在配线间安装布线硬件的墙壁上须覆盖涂有阻燃漆的 $\frac{3}{4}$in（合 1.9cm）厚的木板。
- 在配线间内应至少留有两个为本系统专用的、符合一般办公室照明要求的 220V 电压、10A 单相三极电源插座。

6. 建筑群子系统设计

建筑群子系统也称楼宇管理子系统。一个企业或机关可能分散在几幢相邻建筑物或不相邻建筑物内办公，彼此之间的语音、数据、图像和监控等系统可用传输介质和各种支持设备连接在一起。连接各建筑物之间的传输介质和各种支持设备组成一个建筑群综合布线系统。

1）设计要点

- 建筑群数据网主干线缆一般应选用多模或单模室外光缆。
- 建筑群数据网主干线缆须使用光缆与电信公用网连接时，应采用单模光缆，芯数应根据综合通信业务的需要确定。
- 建筑群主干线缆宜采用地下管道方式进行敷设，设计时应预留备用管孔，以便为扩充使用。

• 当采用直埋方式时,电缆通常铺设在离地面60.96cm以下的地方或按当地法规。

2）建筑群子系统的设计

从技术和方便施工的角度考虑,设计建筑群子系统时需要考虑以下几方面。

(1) 确定电缆系统的一般参数

这些参数包括起止点位置,确认端接点位置,确认涉及的建筑物和每座建筑物的层数,确定每个端接点所需的双绞线对数,确定有多个端接点的每座建筑物所需的双绞线总对数。

(2) 确定建筑物的电缆入口

要确定各个入口管道的位置,每座建筑物有多少入口管道可供使用,入口管道数目是否满足系统的需要。如果建筑物尚未建立,则要根据选定的电缆路由完善电缆系统设计,并标出入口管道的位置。选定入口管理的规格、长度和材料,在建筑物施工过程中安装好入口管道。

(3) 确定主电缆路由和备用电缆路由

对于每一种待定的路由,需要确定可能的电缆结构。所有建筑物共用一根电缆,对所有建筑物进行分组,每组单独分配一根电缆,每座建筑物单用一根电缆,查清在电缆路由中哪些地方需要获准后才能通过,通过比较每个路由的优缺点来选定最佳路由方案。

(4) 选择所需电缆类型和规格

确定电缆长度,画出最终的结构图,画出所选定路由的位置和挖沟详图(包括公用道路图或任何需要经审批才能动用的地区草图),确定入口管道的规格,选择每种设计方案所需的专用电缆,参考《AT&T SYSTIMAX PDS部件指南》有关电缆部分中线号、双绞线对数和长度应符合的有关要求,应保证电缆可进入口管道。如果需用管道,应选择其规格和材料;如果需用钢管,应选择其规格、长度和类型。此外,还要考虑施工环境、施工成本等因素。

3）建筑群子系统中电缆布线方法

(1) 架空布线法

架空安装方法通常只用于现成电线杆,而且电缆的走法不是主要考虑内容的场合,从电线杆至建筑物的架空进线距离不超过30m为宜。建筑物的电缆入口可以是穿墙的电缆孔或管道。入口管道的最小口径为50mm。建议另设一根同样口径的备用管道,如果架空线的净空有问题,可以使用天线杆型的入口。该天线的支架一般不应高于屋顶1 200mm。如果再高,就应使用拉绳固定。此外,天线型入口杆高出屋顶的净空间应有2 400mm,该高度正好使工人可摸到电缆。

通信电缆与电力电缆之间的距离必须符合我国室外架空线缆的有关标准。架空电缆通常穿入建筑物外墙上的U形钢保护套,然后向下(或向上)延伸,从电缆孔进入建筑物内部,电缆入口的孔径一般为50mm,建筑物到最近处的电线杆通常相距应小于30m。

(2) 直埋布线法

直埋布线法优于架空布线法,影响选择此法的主要因素有初始价格、维护费、服务可靠性、安全性、外观等。布线方案选择的原则是既要适用,又要经济,还能可靠地提供服务。直埋布线方案中的细节,如地址的选取、布局的设计等,实际上都是针对每项作业对象专门设计的,是由工程的可行性决定的。

(3) 管道系统布线法

管道系统的设计方法就是把直埋电缆设计原则与管道设计步骤结合在一起。当考虑建

筑群管道系统时，还要考虑接合井。在建筑群管道系统中，接合井的平均间距约180m，或者在主结合点处设置接合井。

（4）隧道内布线法

在建筑物之间通常有地下通道，大多是供暖供水的，利用这些通道来敷设电缆不仅成本低，而且可利用原有的安全设施。例如，考虑到暖气泄漏等情况，电缆安装时应与供气、供水、供暖的管道保持一定的距离，安装在尽可能高的地方，可根据民用建筑设施的有关条例进行施工。

6.2.3 网络工程施工技术

1. 布线工程开工前的准备工作

网络工程经过调研，确定方案后，下一步就是工程的实施，而工程实施的第一步就是开工前的准备工作，要求做到以下几点：

（1）备图：设计综合布线实际施工图，确定布线的走向位置，供施工人员、督导人员和主管人员使用。

（2）备料：网络工程施工过程需要许多施工材料，这些材料有的必须在开工前就备好料，有的可以在开工过程中备料。主要有以下几种：

- 光缆、双绞线、插座、信息模块、服务器、稳压电源、集线器等落实购货厂商，并确定提货日期。
- 不同规格的塑料槽板、PVC防火管、蛇皮管、自攻螺丝等布线用料就位。
- 如果所用设备是集中供电，则准备好导线、铁管和制订好电气设备安全措施（供电线路必须按民用建筑标准规范进行）。
- 制定施工进度表（要留有适当的余地，施工过程中意想不到的事情随时可能发生，并要求立即协调）。

（3）向工程单位提交开工报告。

2. 施工过程中要注意的事项

（1）施工现场督导人员要认真负责，及时处理施工进程中出现的各种情况，协调处理各方意见。

（2）如果现场施工碰到不可预见的问题，应及时向工程单位汇报，并提出解决办法供工程单位当场研究解决，以免影响工程进度。

（3）对工程单位计划不周的问题，要及时妥善解决。

（4）对工程单位新增加的点要及时在施工图中反映出来。

（5）对部分场地或工段要及时进行阶段检查验收，确保工程质量。

（6）制订工程进度表。在制订工程进度表时，要留有余地，还要考虑其他工程施工时可能对本工程带来的影响，避免出现不能按时完工、交工的问题。因此，建议使用督导指派任务表、工作间施工表。

3. 测试

测试所要做的事情有工作间到设备间连通状况，主干线连通状况，信息传输速率、衰减率、距离接线图、近端串扰等因素。

4. 工程施工结束时注意事项

工程施工结束时的注意事项如下：

- 清理现场，保持现场清洁、美观。
- 对墙洞、竖井等交接处要进行修补。
- 各种剩余材料汇总，并把剩余材料集中放置一处，并登记其还可使用的数量。
- 做总结材料。总结材料主要有开工报告、布线工程图、施工过程报告、测试报告、使用报告、工程验收所需的验收报告。

5. 布线中的相关技术

线槽的安装要垂直，无歪斜，整齐牢固。此外，双绞线压接时要一对一对拧开，放入与信息模块相对的端口，注意事项如下：

- 在双绞线压处不能拧，撕开，并防止有断线的伤痕。
- 使用压线工具时，要压实，不能有松动的地方。
- 双绞线开绞不能超过要求。

1）线缆牵引技术

- 将多条线缆聚集成一束，并使它们的末端对齐。
- 用电工带或胶布紧绕在线缆束外面，在末端外绕 50～100mm 长距离。
- 将拉绳穿过电工带缠好的线缆，并打好结。

2）布线技术

布线包括建筑物间布线和建筑物内布线，建筑物内布线包括暗道布线、天花板顶内布线、墙壁线槽布线。布线的要点如下：

（1）管道（或桥架）内穿放电缆时，直线管路的管径利用率一般为 50%～60%；弯管路的管径利用率一般为 40%～50%。

（2）金属电线管、金属软管、金属桥架及配线架均需整体连接后接地。弯管路的中心夹角不应小于 90°；电缆穿放中，避免过紧地缠绕电缆，不要损坏线缆的外皮，不要切断缆内导线；在牵引和捆绑电缆时应消除线缆中的应力（垂直布放的干缆，必须每隔 1.5m 将电缆固定在梯级电缆桥架上）。

（3）根据配线间内需要放置网络设备的供电要求，在配备 IDF 的配线间内必须配置 2 个以上 220V 电源插座，在条件允许时，可配备 UPS 不间断电源。

（4）施工人员必须遵照电缆色码接续，穿线时每根电缆都必须在两头做出相同的标记，并与施工图吻合。电源线与 PDS 管线尽量减少交叉，两管交叉时应相距 5cm 以上，两管并行时应相距 15cm 以上。

（5）配线架的安装位置和所占墙面空间须按设计图纸要求而定。建议在配线架的安装墙面上先固定一块 2cm 厚涂有防火漆的木板，以便安装。应注意光纤布线的传输质量和光纤 ST 连接头的制作质量。因此，在光纤布放须弯曲时不能超过最小弯曲半径：安装时为光纤直径的 20 倍；安装后为光纤直径的 10 倍。敷设光纤牵引力不能超过最大敷设张力。

6.2.4 网络工程的验收

在进行网络工程验收之前，应做好前期准备，例如要确保综合布线（光缆和双绞线）通过了认证测试（测试报告），确保布线进行了标识，确保设备的连接跳线合格（或经过了测试），

同时，不要忽视各种跳线。网络验收的前期准备工作具体如下：

- 所有网络关键设备及其应用软件必须全部连通运行。
- 避免一些备份设备日后开通对网络的影响。
- 网络的站点应该尽可能地全部上网。
- 确保各个站点对网络的影响(通断、性能等)。
- 尽可能将所有主机连接上网，测试网络实际承载能力。
- 准备网络设计的图纸。
- 确认实际网络和设计的对比。

验收的内容包括网络拓扑图、网络规划信息、网络设备信息备案、正常运行时网络重点端口的流量(网络基准测试)路由器或交换机端口流量趋势图、流量趋势备案、正常运行时网络协议和繁忙用户的分布统计、网络的吞吐能力或加载测试(路由和交换能力)等内容，详细项目和内容如表 6-1 所示。

表 6-1　综合布线系统系统工程验收项目及内容

阶　段	验收项目	验收内容	验收方式
施工前检查	环境要求	(1) 土建施工：地面、墙面、门、电源插座及接地装置 (2) 土建工艺：机房面积、预留孔洞 (3) 施工电源 (4) 活动地板敷设	施工前检查
	器材检验	(1) 外观检查 (2) 规格、品种、数量 (3) 电缆电气性能抽样测试 (4) 光纤特性测试	施工前检查
	安全、防火要求	(1) 消防器材 (2) 危险物的堆放 (3) 预留孔洞防火措施	施工前检查
设备安装	设备机架	(1) 规格、程式、外观 (2) 安装垂直、水平度 (3) 油漆不得脱落，标志完整齐全 (4) 各种螺钉必须紧固 (5) 防震加固措施 (6) 接地措施	随工检验
	信息插座	(1) 规格、位置、质量 (2) 各种螺钉必须拧紧 (3) 标志齐全 (4) 安装符合工艺要求 (5) 屏蔽层可靠连接	随工检验
楼内电、光缆布放	电缆桥架及槽道安装	(1) 安装位置正确 (2) 安装符合工艺要求 (3) 接地	随工检查
	缆线布放	(1) 缆线规格、路由、位置 (2) 符合布线缆线工艺要求	随工检验

续表

阶　　段	验 收 项 目	验 收 内 容	验 收 方 式
楼间电、光缆布放	架空缆线	(1) 吊线规格、架设位置、装设规格 (2) 吊线垂度 (3) 缆线规格 (4) 卡、挂间隔 (5) 缆线的引入符合工艺要求	随工检验
	管道缆线	(1) 使用管孔孔位 (2) 缆线规格 (3) 缆线走向 (4) 缆线的防护设施的设置质量	隐蔽工程签证
	埋式缆线	(1) 缆线规格 (2) 敷设位置、深度 (3) 缆线的防护设施的设置质量 (4) 回土夯实质量	隐蔽工程签证
	隧道缆线	(1) 缆线规格 (2) 安装位置、路由 (3) 土建设计符合工艺要求	隐蔽工程签证
	其他	(1) 通信线路与其他设施的间距 (2) 进线室安装、施工质量	隐蔽工程签证
线缆终端	信息插座	符合工艺要求	随工检验
	配线模块	符合工艺要求	随工检验
	光纤插座	符合工艺要求	随工检验
	各类跳线	符合工艺要求	随工检验
系统测试	工程电气性能测试	(1) 连接图 (2) 长度 (3) 衰减 (4) 近端串扰 (5) 设计中特殊规定的测试内容	竣工检验
	光纤特性测试	(1) 类型(单模或多模) (2) 衰减 (3) 反射	竣工检验
	系统接地	符合设计要求	竣工检验
工程总验收	竣工技术文件	清点、交接技术文件	竣工检验
	工程验收评价	考核工作质量,确认验收结果	竣工检验

6.3　数据库管理

数据库管理是有关建立、存储、修改和存取数据库中信息的技术,是为保证数据库系统的正常运行和服务质量,有关人员须进行的技术管理工作。数据库管理的主要内容有数据库的建立、调整、重组、重构、安全控制,数据的完整性控制和对用户提供技术支持。本节主要以 SQL Server 数据库安全为主介绍数据库的管理操作,其他内容的基本管理请参考相关文献。

6.3.1 SQL Server 系统安全管理

数据的安全性管理是数据库管理系统应实现的重要功能之一。SQL Server 数据库采用了对用户登录进行身份认证和对用户进行的操作进行权限控制两种安全管理机制。用户要对某一数据库进行操作，必须满足以下 3 个条件：

- 登录 SQL Server 服务器时必须通过身份验证。
- 必须是该数据库的用户，或者是某一数据库角色的成员。
- 必须有执行该操作的权限。

1. 用户账户管理

1）Windows 身份验证登录账号的建立

该模式可以通过调用存储过程和企业管理器建立 Windows NT 认证模式的登录账号，以企业管理器为例：

(1) 创建 Windows Server 2003 的用户：以管理员身份登录到 Windows Server 2003，选择“开始”→“所有程序”→“管理工具”→“计算机管理”命令，在弹出的对话框中选择“本地用户和组”。继续右击“用户”图标，在快捷菜单中选择菜单项“新用户”，然后按提示输入用户名、密码，单击“创建”按钮，然后单击“关闭”按钮。

(2) 将 Windows 网络账号加入到 SQL Server 中：以管理员身份登录到 SQL Server，进入企业管理器，右击“登录”图标，在出现的快捷菜单中选择“新建登录”，出现如图 6-17 所示的对话框，单击“常规”选项卡的“浏览”按钮，可选择用户名或用户组添加到 SQL Server 登录用户列表中。

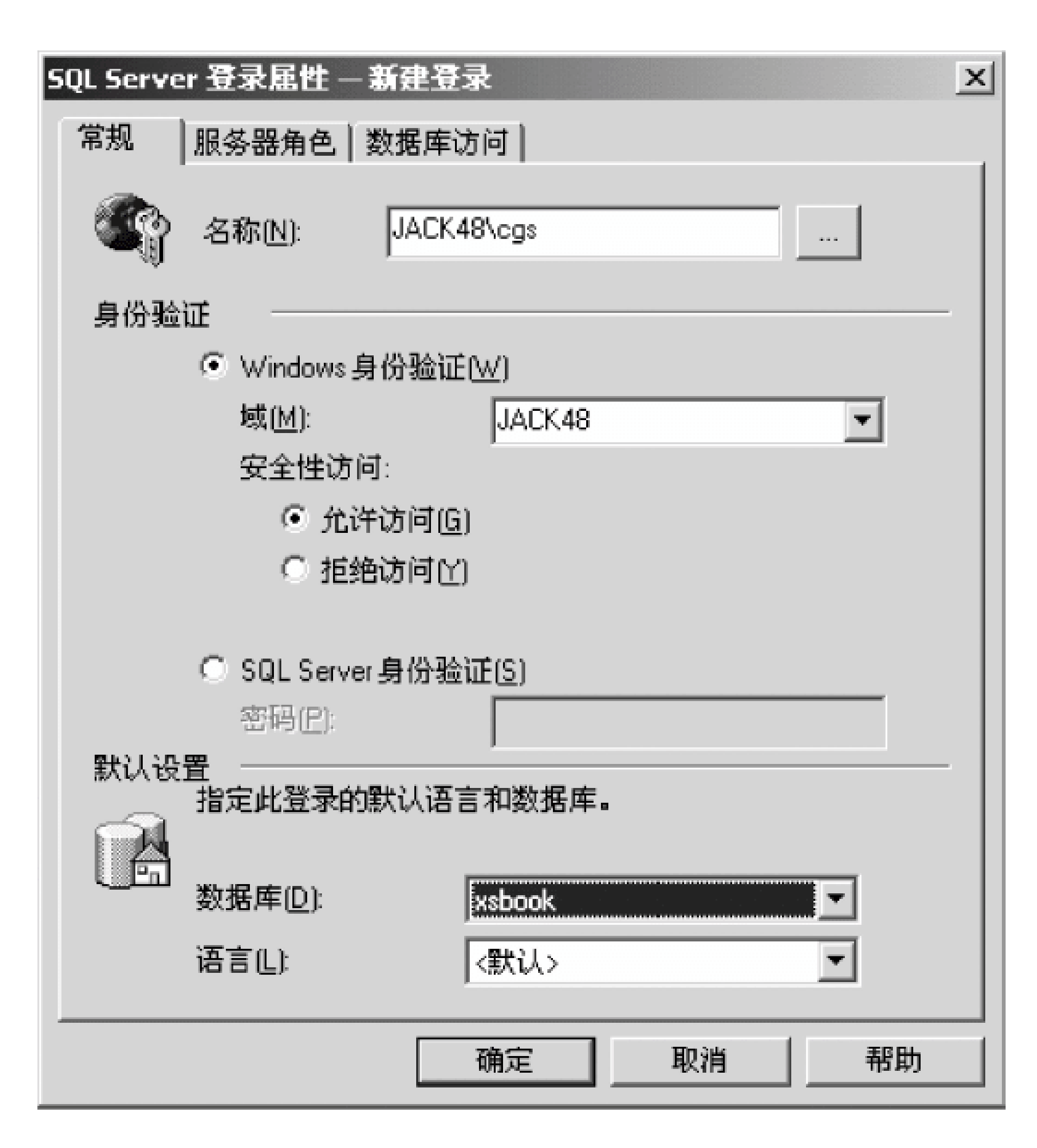


图 6-17　Windows 身份验证模式账号的建立

2）混合认证模式下 SQL Server 登录账号的建立

(1) 在企业管理器中，选择要登录的 SQL Server 服务器图标并右击，在出现的快捷菜单中选择菜单项“属性”。

（2）在弹出的 SQL Server 服务器属性配置对话框中，选择“安全性”选项卡，选择身份验证方式为“SQL Server 与 Windows”，然后单击“确定”按钮。

（3）在企业管理器中选择“登录”图标并右击，在快捷菜单中选择“新建登录”命令。

（4）在弹出的如图 6-18 所示的对话框中选择“SQL Server 身份验证”方式，然后输入名称、密码，单击“确定”按钮。

2. 服务器角色与数据库角色

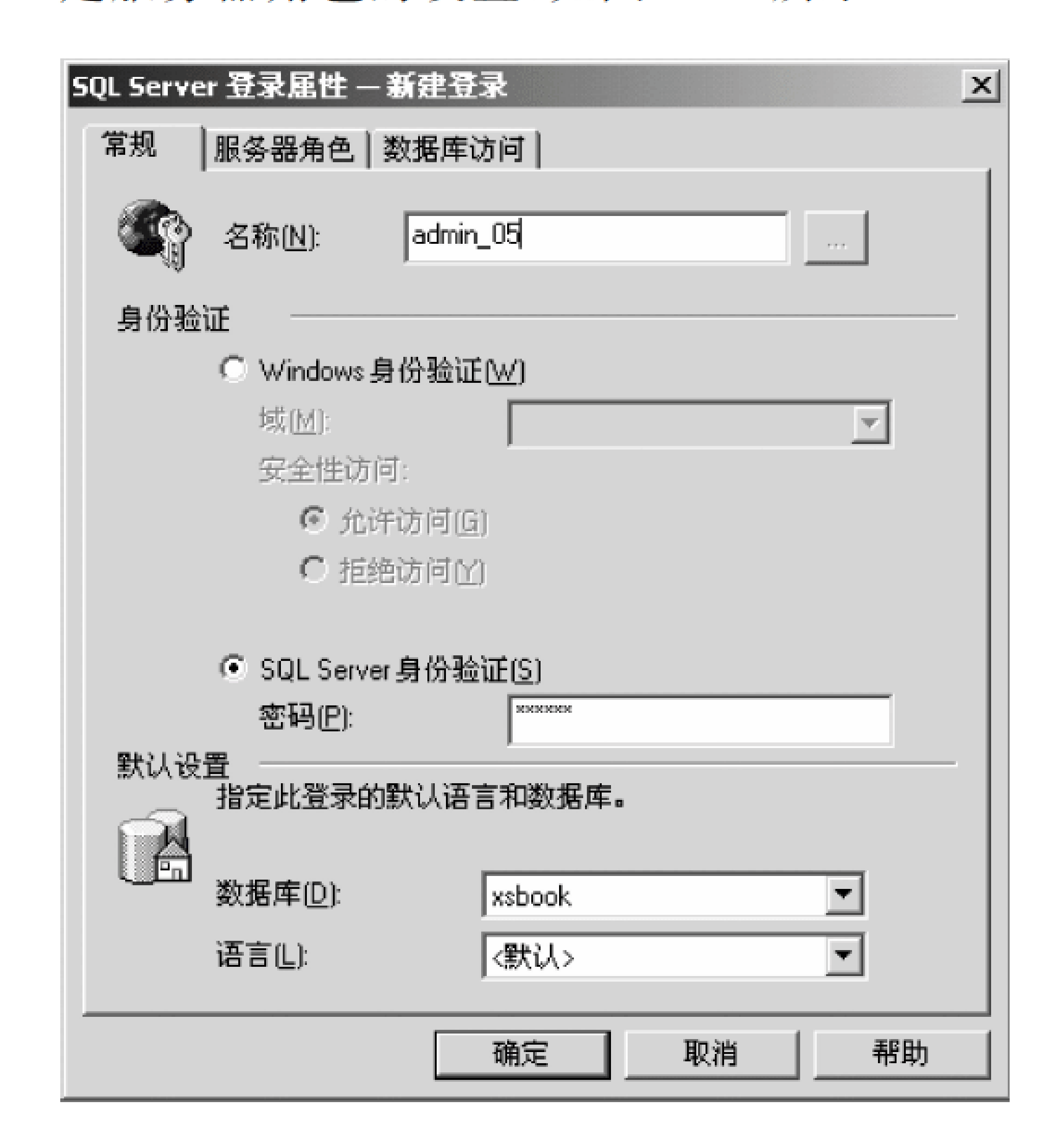
在 SQL Server 中，通过角色可将用户分为不同的类，对相同类用户（相同角色的成员）进行统一管理，赋予相同的操作权限，SQL Server 给用户提供了预定义的服务器角色（固定服务器角色）和数据库角色（固定数据库角色），固定服务器角色和固定数据库角色都是 SQL Server 内置的，不能进行添加、修改和删除。用户可根据需要，创建自己的数据库角色。

1）固定服务器角色的管理

服务器角色独立于各个数据库，如果在 SQL Server 中创建一个登录账号后，要赋予该登录者具有管理服务器的权限，此时可设置该登录账号为服务器角色的成员。

（1）以系统管理员身份登录到 SQL Server 服务器，在登录图标对应的列表框中，选择登录账号（本例为“JACK48\cgs”）的项目双击。

（2）选择“服务器角色”选项卡，选项卡中列出了 SQL Server 所有的固定服务器角色，将“System Administrators”服务器角色前的复选框选中，然后单击“确定”按钮即可完成固定服务器角色的设置，如图 6-19 所示。



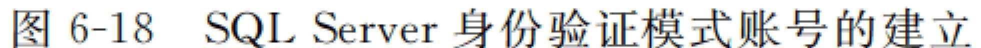

图 6-18　SQL Server 身份验证模式账号的建立



图 6-19　SQL Server“服务器角色”选项卡

2）固定数据库角色的管理

固定数据库角色定义在数据库级别上，并且有权进行特定数据库的管理及操作，SQL Server 提供了以下固定数据库角色：

- db_owner：数据库所有者，可执行数据库的所有管理操作。

- db_accessadmin：数据库访问权限管理者，具有添加和删除数据库使用者、数据库角色和组的权限。
- db_securityadmin：数据库安全管理员，可管理数据库中的权限，如设置数据库表的插入、删除、修改和查询等存取权限。
- db_ddladmin：数据库 DDL 管理员，可增加、修改或删除数据库中的对象。
- db_backupoperator：数据库备份操作员，具有执行数据库备份的权限。
- db_datareader：数据库数据读取者。
- db_datawriter：数据库数据写入者，具有对表进行插入、删除和修改的权限。
- db_denydatareader：数据库拒绝数据读取者，不能读取数据库中任何表的内容。
- db_denydatawriter：数据库拒绝数据写入者，不能对任何表进行插入、删除和修改操作。
- public：是一个特殊的数据库角色，每个数据库用户都是 public 角色的成员，因此，不能将用户、组或角色指派为 public 角色的成员，也不能删除 public 角色的成员。

3）用户自定义数据库角色

（1）创建数据库角色：以系统管理员身份登录 SQL Server，并进入企业管理器，选中目录树数据库（本例为 XSBOOK）结点的“角色”图标并右击，在弹出的快捷菜单中选择“新建数据库角色”，进入如图 6-20 所示的对话框，输入角色名，单击“确定”按钮。

（2）创建数据库用户并加入数据库角色：即在某一数据库中为 SQL Server 服务器的登录账号或 Windows NT 的登录账号创建一数据库用户账号，将数据库用户加入该数据库中的某一角色，即使数据库用户成为某一角色的成员。

在企业管理器目录树中，选择 XSBOOK 数据库下的“用户”图标并右击，在出现的快捷菜单中选择“新建数据库用户”，进入如图 6-21 所示的对话框，选择登录名，选中该用户所加入的数据库角色，然后单击“确定”按钮可将 cgs 创建为数据库 XSBOOK 的用户，并添加到数据库 admin_role 角色中。

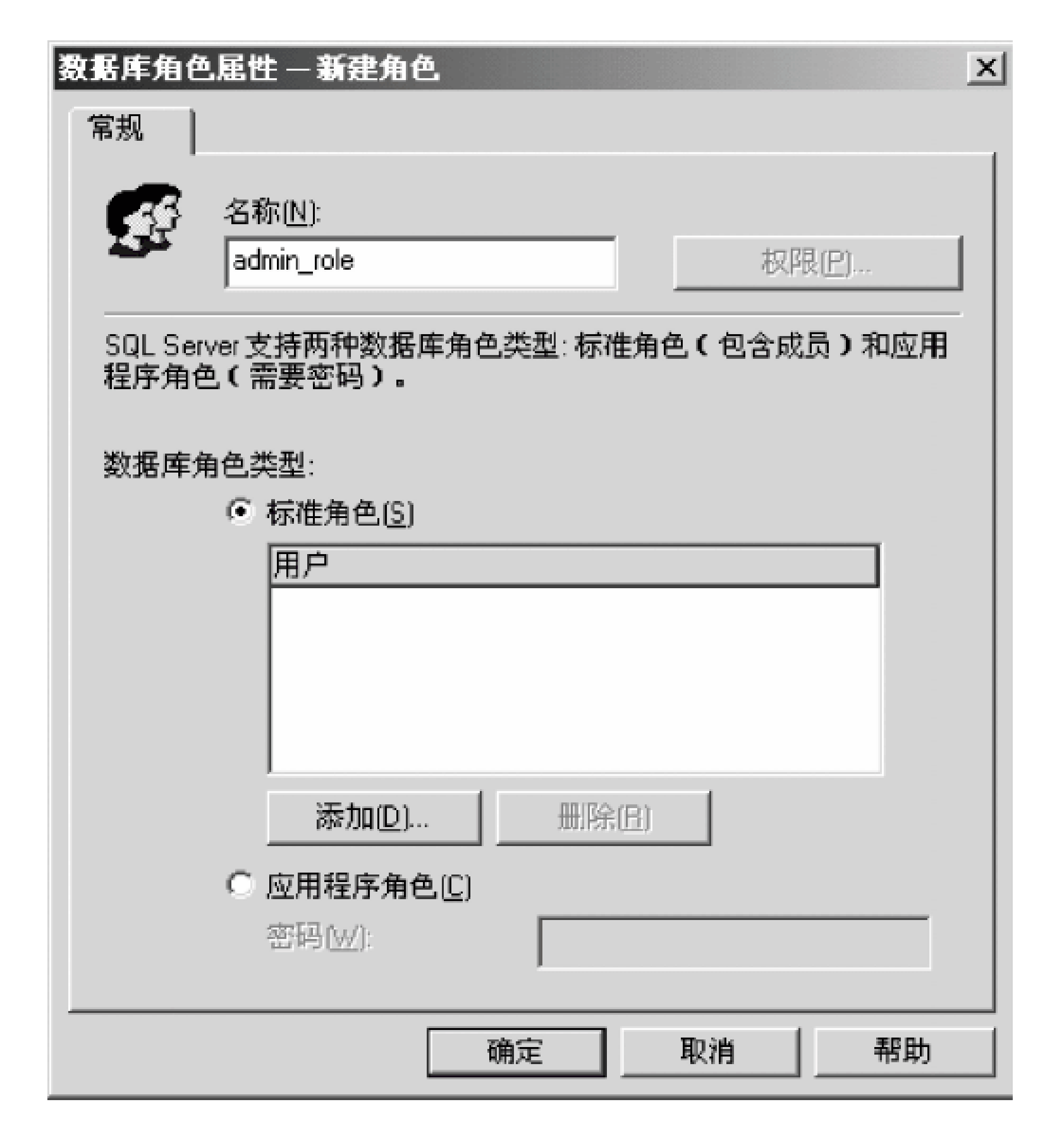


图 6-20 “数据库角色属性”对话框



图 6-21 “数据库用户属性”对话框

(3) 给数据库角色赋予创建数据库对象的权限：在企业管理器目录树中，选择 XSBOOK 数据库节点右击，在快捷菜单中选择“属性”命令，进入如图 6-22 所示的对话框，选择“权限”选项卡，选中允许数据库角色或数据库用户执行的权限。

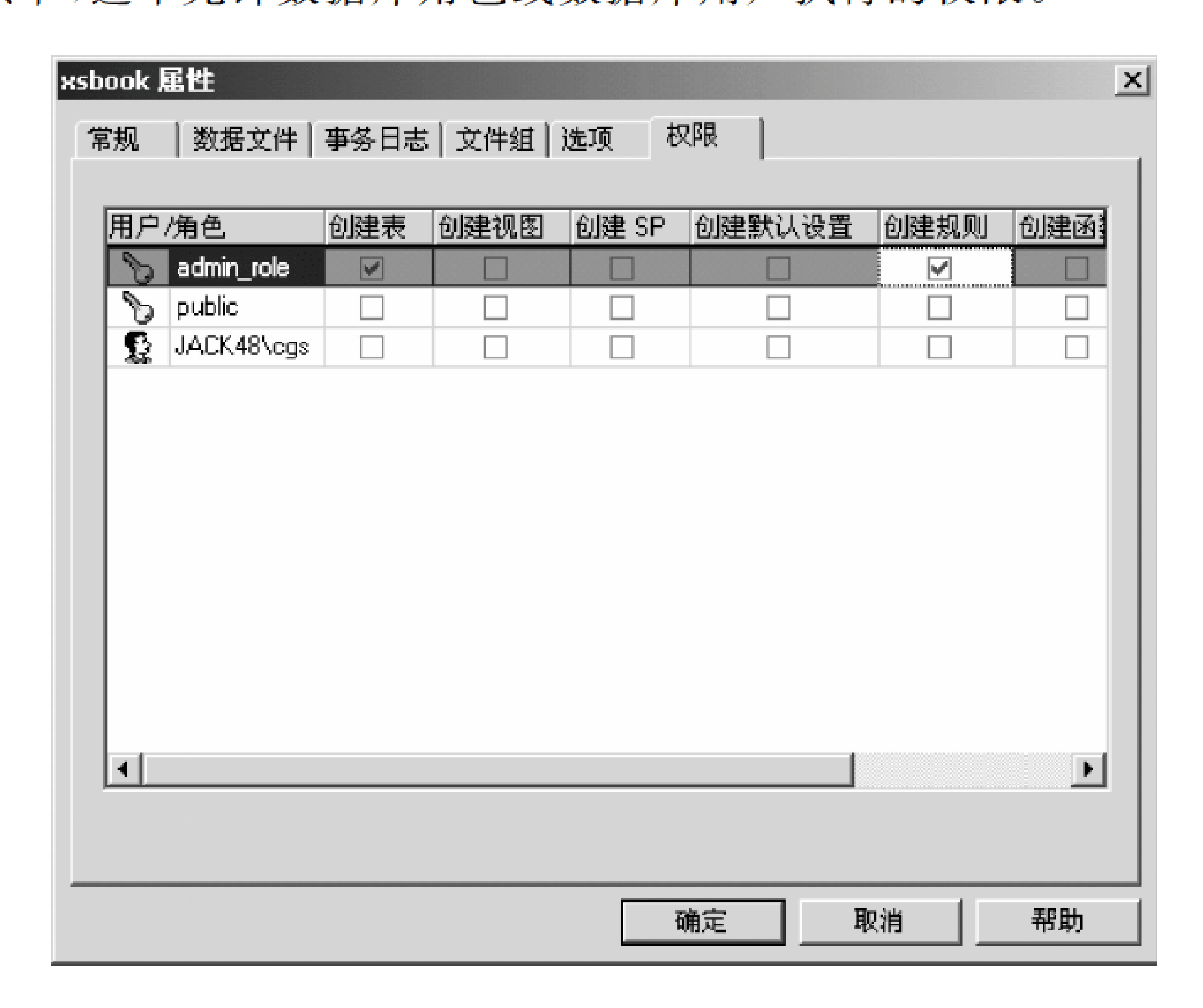


图 6-22 “权限”选项卡

(4) 给数据库角色赋予表操作权限：在企业管理器的目录树中，双击 XSBOOK 数据库节点下角色图标的项目“admin_role”，弹出如图 6-23 所示的对话框。



图 6-23 “数据库角色属性”对话框

(5) 单击“权限”按钮，根据允许的操作可设置相应的权限，如图 6-24 所示。单击“列”按钮可以继续设置列操作权限。



图 6-24 “权限”选项卡

6.3.2 数据库备份和还原管理

数据库备份/恢复可以使用备份/恢复命令、使用企业管理器和使用向导等多种方法，以企业管理器为例方法为：

1. 备份数据库

(1) 打开 SQL Server 企业管理器，展开 SQL Server 组 Local 下的数据库，右击要备份的数据库，在弹出的快捷菜单中选择“所有任务”下的“备份数据库”命令。

(2) 在弹出的“备份数据库”对话框中，单击“添加”按钮，填写备份文件的路径和文件名，单击“确定”按钮添加备份文件，单击“备份”对话框上的“备份”按钮，即可开始进行备份。

2. 还原数据库

(1) 打开“SQL Server”的企业管理器，打开数据库，右击“数据库”，打开“所有任务”里面“还原数据库”命令，如图 6-25 所示。

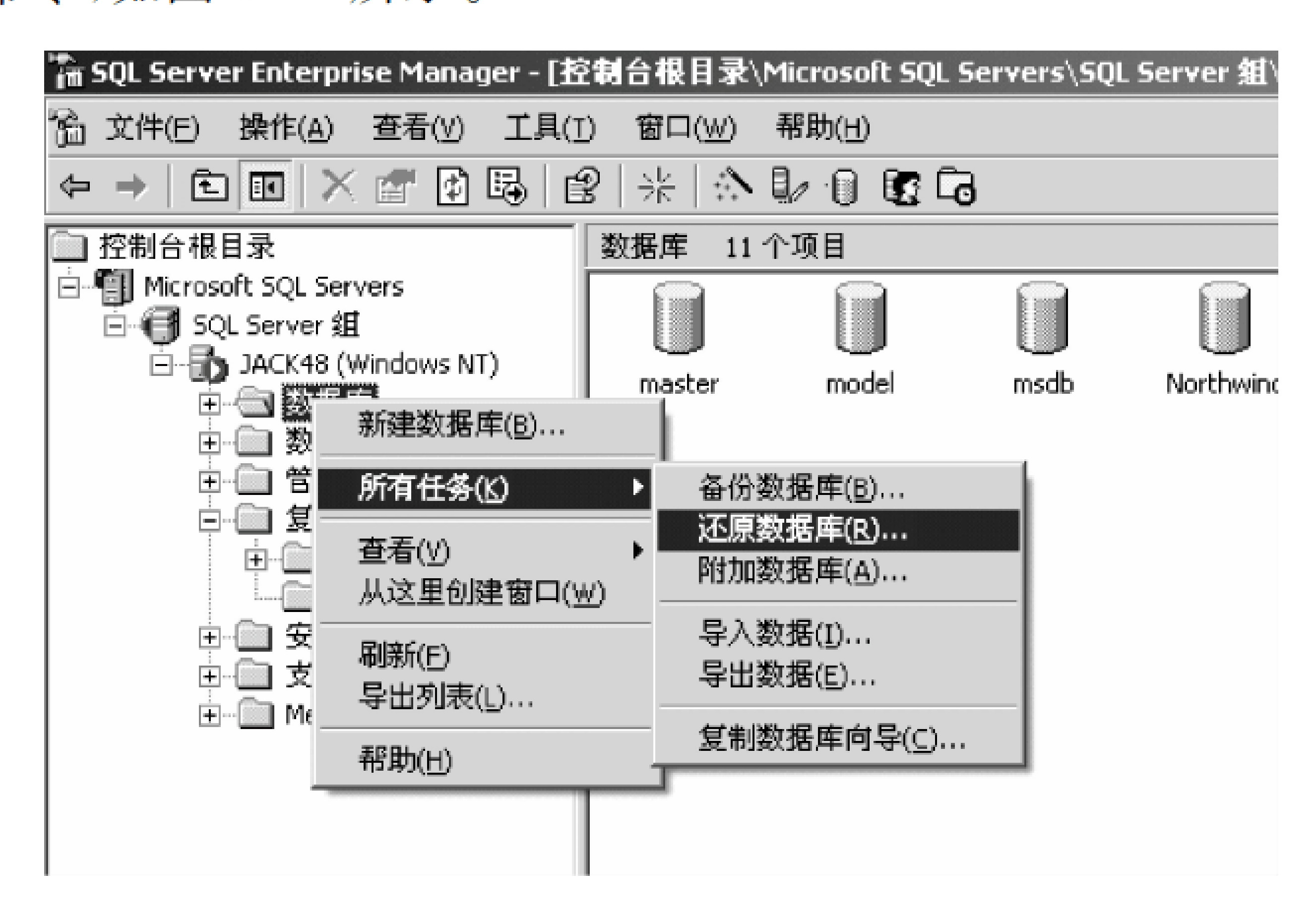


图 6-25 选择“还原数据库”命令

(2) 在如图 6-26 所示的对话框中,命名自己要还原的数据库名字,单击“从设备”单选按钮,然后单击“选择设备”按钮。



图 6-26 “还原数据库”对话框

(3) 在弹出的对话框中单击“添加”按钮,找到备份文件夹的路径,选择需要还原的备份数据库,如图 6-27 所示。



图 6-27 “选择还原设备”对话框

(4) 从设备选择好备份文件后,单击“确定”按钮进行数据库还原。

6.3.3 数据库维护计划

(1) 打开企业管理器后,选择“管理”→“数据库维护计划”,然后右击,从快捷菜单中选择“新建维护计划”命令,如图 6-28 所示。

图 6-28　选择“新建维护计划”命令

(2) 根据向导提示，在弹出的对话框中选择需要备份的数据库，只需要勾选要备份的数据库即可。

(3) 数据优化信息设置：数据库存在预留空间，使用此设置在备份时可以将预留的空间删除，避免空间浪费；执行此操作的时间可以在“调度”列表框里更改，如图 6-29 所示。

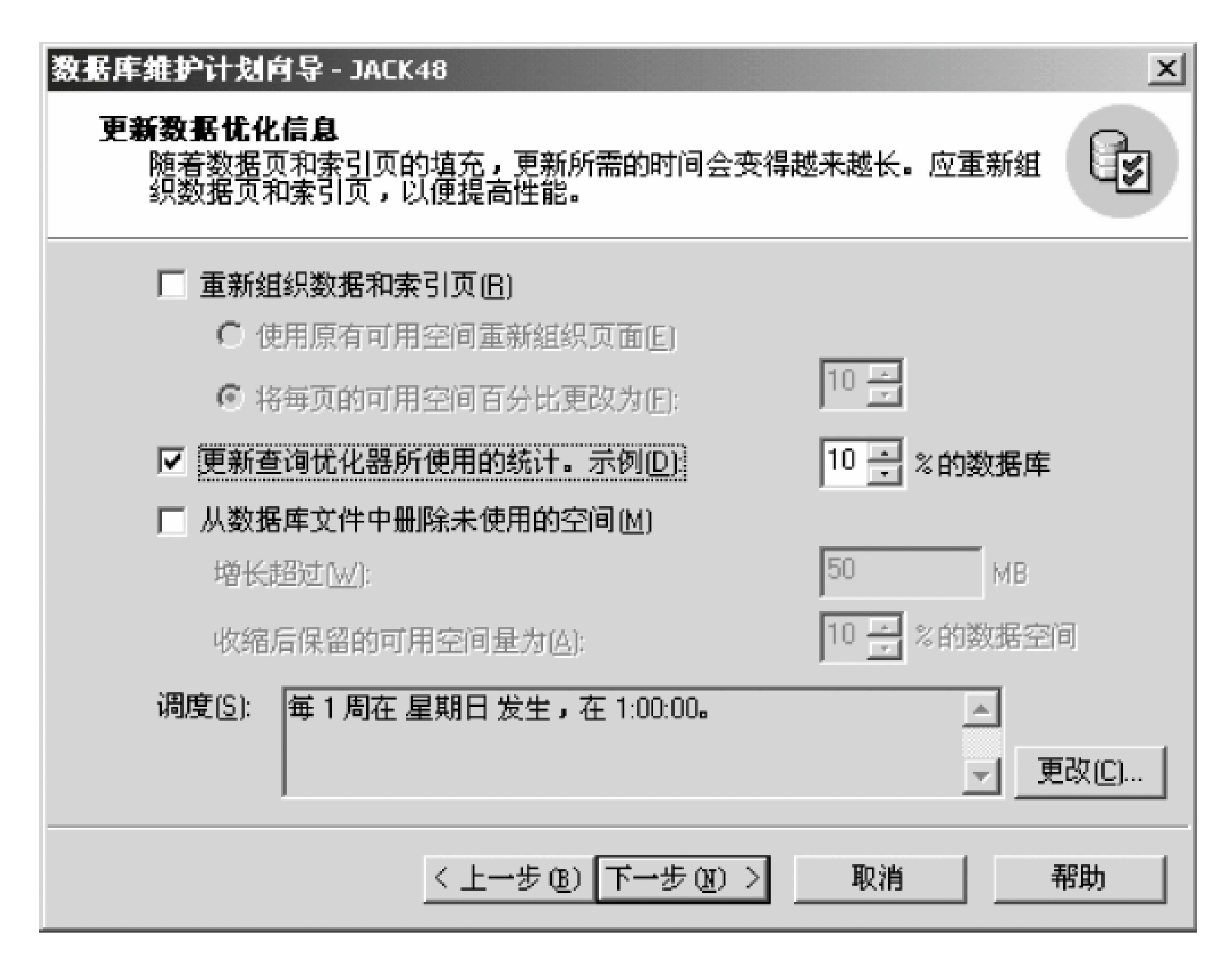


图 6-29　“更新数据优化信息”对话框

(4) 数据库完整性检查设置：此设置是防止软硬件出问题导致备份出现差异而进行检查；执行时间也是在“调度”列表框里设置，如图 6-30 所示。

(5) 设置数据库存放方式、备份时间(调度设置备份周期)，如图 6-31 所示。

(6) 选择数据库备份存放的路径以及自动删除早期备份文件、删除周期，如图 6-32 所示。

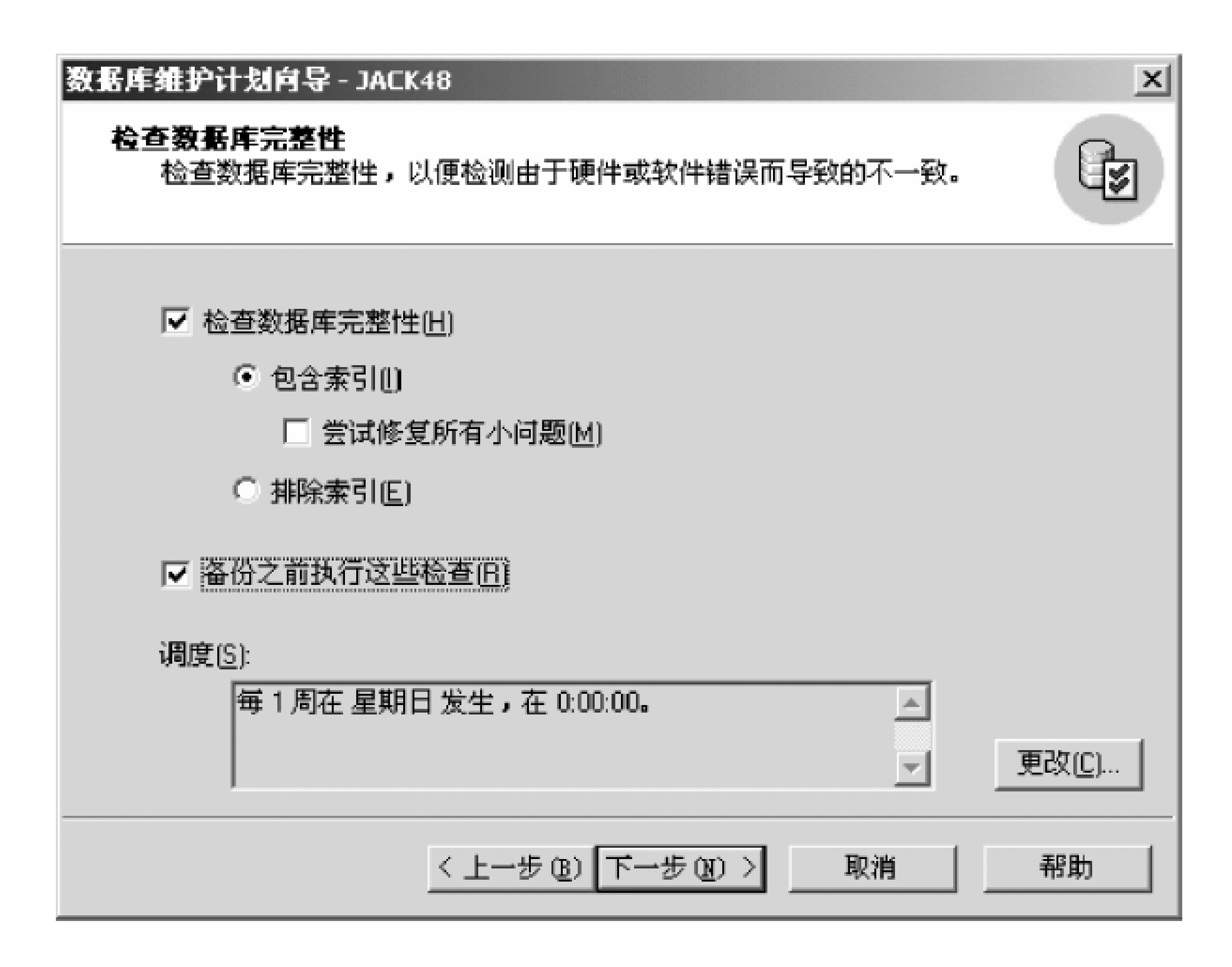


图 6-30 “检查数据完整性”对话框

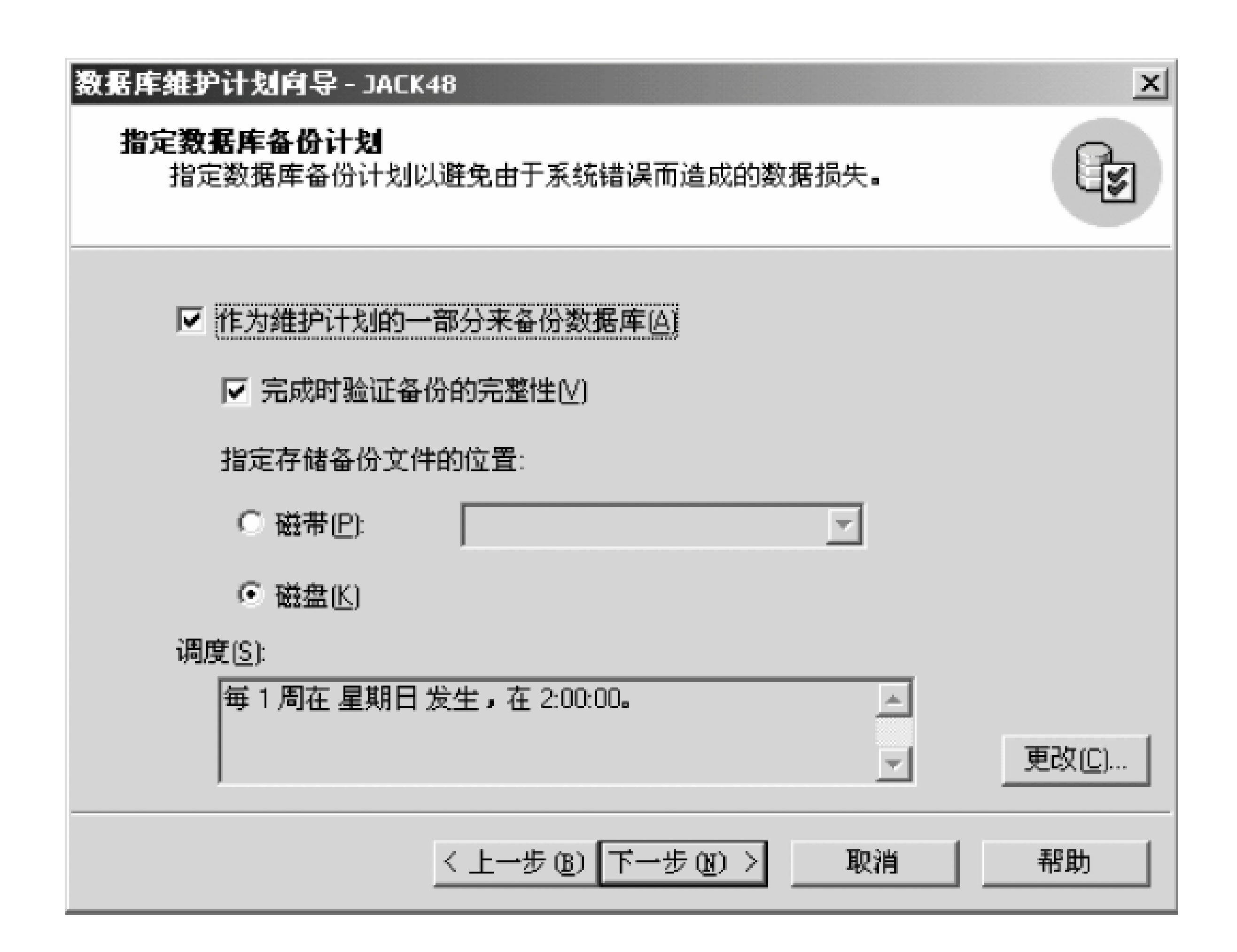


图 6-31 “指定数据库备份计划”对话框

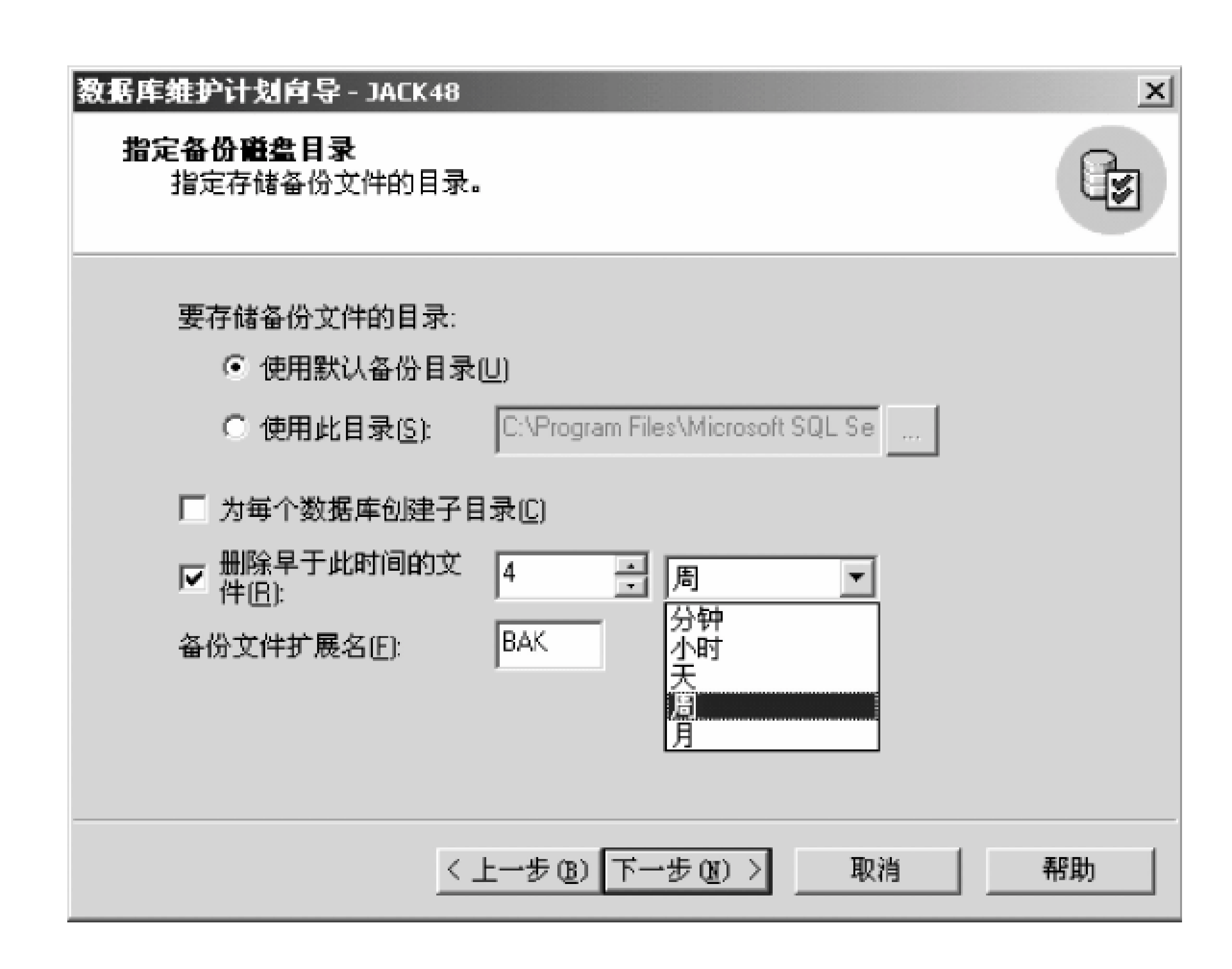


图 6-32 “指定备份磁盘目录”对话框

(7) 报表、历史记录均可以不用设置,如有需要用户可以自行设置;填写备份计划名称,单击"完成"按钮,完成备份计划。

6.3.4 代理服务

在 SQL Server 数据库管理中,可以通过 SQL Server 代理服务来自动执行周期性的工作。SQL Server 代理服务能够自动执行管理员安排的每天必须进行的固定不变的任务,还可以在服务器发生异常事件的时候,自动发出通知,以便让操作人员及时获得信息,并作出处理。如上一节中创建的"数据库维护计划",就需要启动 SQL Server 代理才能执行。

SQL Server 代理服务由作业、操作员和警报 3 个部分组成。

1. 作业

作业是可以由 SQL Server 代理调度执行一次或多次的管理任务,SQL Server 代理可以监视作业在执行时是成功还是失败。作业既可以在本地服务器上执行,也可以在远程服务器上执行。管理员可以为作业安排执行的时间表,代理将按照这一时间表自动调度作业的执行。

一个作业是由一个或多个作业步骤组成的,作业步骤既可以是可执行程序,也可以是 Windows Server 2003 命令、T-SQL 语句、ActiveX 脚本或复制代理等。作业要在多台服务器上执行,需要设置主服务器和目标服务器。定义作业需要指定以下属性:名称、类别、拥有者、描述、作业步骤、调度时间表、完成通知等。创建作业的过程如下。

(1) 在企业管理器中展开"管理"→"SQL Server 代理" →"作业",然后右击"作业",在弹出的快捷菜单中选择"新建作业"命令。

(2) 在"常规"选项卡中输入作业名,在"步骤"选项卡中单击"新建"按钮,在"新建作业步骤"对话框中输入步骤名、类型、数据库和命令,如图 6-33 所示。

(3) 单击"确定"按钮完成步骤的定义。"调度"和"通知"根据实际情况进行设置即可。

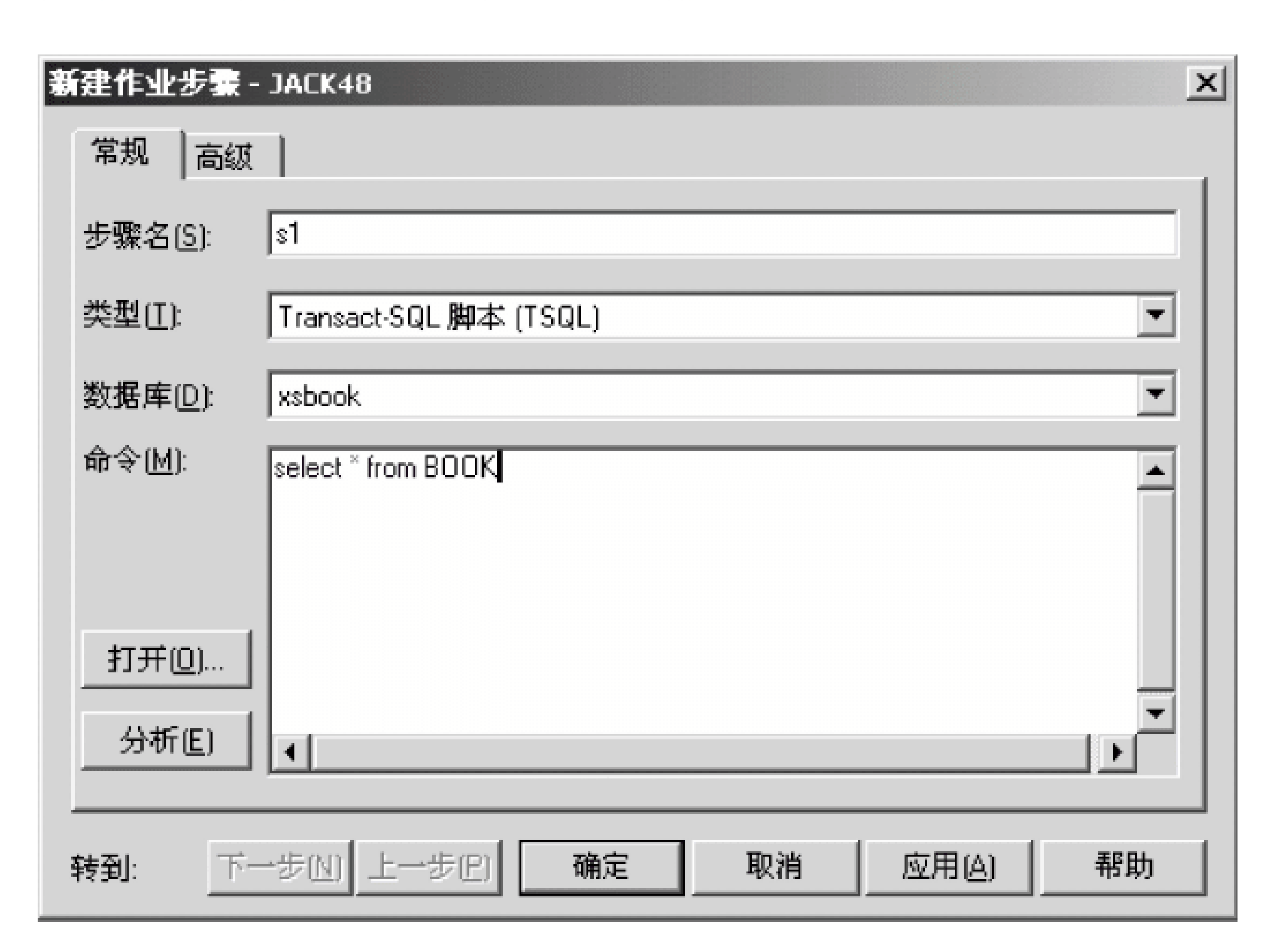


图 6-33 "新建作业步骤"对话框

2. 操作员

操作员是负责维护 SQL Server 服务器运行的个人。当 SQL Server 出现异常时,需要通知操作员。操作员可以通过电子邮件、第三方的呼叫软件、Net send 命令等方式获得通知。

3. 警报

警报定义了当在 SQL Server 中特定的事件发生时，SQL Server 应该做出的反应。警报可以通过通知操作员，将事件转发到其他服务器，执行一个作业方式响应 SQL Server 事件。创建警报的对话框如图 6-34 所示。默认情况下，SQL Server 自动响应用程序日志文件中写入的如下事件：

- 严重级别大于等于 19 的事件。
- 使用带有 WITH LOG 的 RAISERROR 语句产生的事件。
- 由 xp_logevent 存储过程记录的应用程序事件。

只有在定义了警报后，才可以对操作员发出通知。警报的主要内容包括警报名称和触发警报的事件或警报执行的服务器性能条件。



图 6-34 “新建警报属性”对话框

6.4 资源管理

6.4.1 网络资源管理概述

1. 网络资源

网络资源包括物理资源和逻辑资源。管线网、电缆网、光缆网、机房等基础设施是物理资源，通过对网络的调度和配置，形成了通道、电路等逻辑资源。网络资源管理就是企业对所拥有的全部物理、逻辑网络以及连接这些网络的节点的管理。

2. 网络资源管理的意义

网络资源是企业业务流程中不可忽视的基础，它是业务开通和业务保障这两个关键业务流程实现自动化的重要前提。网络资源管理可以实现对全网资源进行系统的统筹，保证业务的配置被正确地反映到网络资源上。当网络发生故障时，维护部门可以迅速定位、排除故障，同时对被影响的业务与客户状况了如指掌，直接大幅提高服务质量。

3. 网络资源管理中存在的问题

- 缺乏统一、规范的网络资源信息描述与存储，资源信息没有完整统一的定义。
- 网络资源信息分散，各个部门对网络资源的管理范围界定不清。
- 对网络资源使用状况缺乏有效的监控、校核机制和统一的调度流程控制。

所以，建立集中统一的网络资源管理平台已经成为企业网络资源管理最迫切的基础建设任务。

4. 网络资源管理系统

网络资源管理系统是整个网络资源统一管理的平台，主要功能是实现整个网络资源的统一管理、统一维护、统一调度。采用网络资源管理系统能够帮助企业提高经济效益。目前的网络资源管理系统主要集中在电信部门，主要产品有 ZSmart ResMaster、BOCO_NetPilot v3. x、NetTracker 等。网络资源管理系统主要包括 4 大功能模块：

- 网络资源管理模块——动态管理网络中各种物理资源（局站、机房、设备、管道、DDF、ODF 等）和逻辑资源（PDH、SDH、DWDM、电路等），并结合 GIS 对资源对象进行定位。
- 资源调度管理模块——规范资源调度全流程，实现对电路等网络资源闭环调度管理功能，并能通过 Web 方式申请调度资源。
- 资源预测分析模块——系统能对各种网络资源进行预测分析，预测分析结果可通过客户端或者 Web 方式展示，也可以各种形式输出，并可按用户需求定制各种报表。
- 系统自身管理模块——包括安全管理、日志管理、数据备份与恢复和基础数据配置功能。

6.4.2 物理资源管理

企业中常用的物理资源包括网卡、交换机、集线器、路由器、防火墙、UPS、测试设备、存储设备、VPN 设备、打印服务器、光纤设备等。由于大部分内容在前面的章节中已经介绍或基本熟悉，所以就不赘述了。本节主要介绍 Windows Server 2003 基本存储资源的管理，包括磁盘分区和卷的管理、磁盘配额和磁盘的日常维护管理等内容。

1. 基本磁盘与动态磁盘

无论是操作系统还是数据都存储在容量固定且非常脆弱的磁盘上。因此，能否合理地分配磁盘空间，能否监控磁盘正常运转，能否确保数据不会丢失，就显得非常重要。这不仅关系到操作系统能否稳定运行，而且关系到比那些硬件设备更为宝贵的数据资源是否安全。

Windows Server 2003 将磁盘存储类型分为基本磁盘和动态磁盘两种。一个硬盘既可以是基本的，也可以是动态的，但不能既是基本的又是动态的，在同一个磁盘上不能组合多种存储类型。在基本磁盘上，使用分区来分割磁盘；在动态磁盘上，将存储分为卷而不是分区。

在 Windows Server 2003 中，硬盘自动初始化为基本磁盘。基本磁盘的管理包括创建主要磁盘分区，创建扩展磁盘分区，磁盘分区的格式化，加卷标，转换文件系统，删除、更改驱动器号等。动态磁盘的管理是基于卷的管理，卷是一个或多个磁盘上的可用空间组成的存

储单元，可以将它格式化为一种文件系统并分配驱动器号。动态磁盘上的卷可以具有下列任意一种布局方式：简单卷、跨区卷、带区卷、镜像卷或 RAID-5 卷，它们提供容错、提高磁盘利用率和访问效率的功能。

2. 卷的管理

1）简单卷

简单卷由单个物理磁盘上的磁盘空间组成，它可以由磁盘上的单个区域或者由多个连续的区域组成。创建简单卷的具体操作步骤如下：

（1）在“磁盘管理”中，右击一块未指派空间的物理磁盘，从快捷菜单中选择“新建卷”命令。

（2）在“选择卷类型”对话框中，选择“简单”单选按钮，然后单击“下一步”按钮。

（3）在“选择磁盘”对话框中，设置简单卷的大小。

（4）在“指派驱动器号和路径”对话框中，为该简单卷指派一个驱动器名。

（5）单击“完成”按钮，系统将对该卷格式化，完成简单卷的建立。

2）跨区卷

跨区卷由多个磁盘上的可用空间组成，也就是将多个物理磁盘的未指派空间合并为一个逻辑盘，用一个逻辑驱动器表示。跨区卷的创建步骤如下：

（1）在“磁盘管理”中，右击一块未指派空间，从快捷菜单中选择“新建卷”命令。

（2）在“选择卷类型”对话框中，选择“跨区”单选按钮，单击“下一步”按钮。

（3）在“选择磁盘”对话框中，从磁盘 1、2 分别选择可用的容量，然后，单击“下一步”按钮。

（4）在“指派驱动器号和路径”对话框中，为该跨区卷指派一个驱动器名。

（5）在弹出的“卷区格式化窗口”对话框中，选择格式化参数，然后单击“下一步”按钮。

（6）单击“完成”按钮，即可完成跨区卷的建立。

3）带区卷

带区卷是由 2 个或多个磁盘（最多 32 块磁盘）中的空余空间组成的卷，在向带区卷中写入数据时，数据被分割成 64KB 的数据块，然后同时向阵列中的每一块磁盘写入不同的数据块。这个过程显著提高了磁盘效率和性能，但是，带区卷不提供容错性。创建带区卷的方法如下：

（1）在“磁盘管理”中，右击未分配的空间，从快捷菜单中选择“创建卷”命令。

（2）在“新建卷向导”中，单击“下一步”按钮，选择“带区”单选按钮并单击“下一步”按钮。

（3）选择想使用的磁盘和输入在每块磁盘中分配给该卷的空间，并单击“下一步”按钮。然后根据向导指示完成相应操作。

4）镜像卷

镜像卷可以将用户的相同数据同时复制到两个物理磁盘中。如果一个物理磁盘出现故障，虽然该磁盘上的数据将无法使用，但系统仍能够继续使用尚未损坏而仍继续正常运转的磁盘进行数据的读写操作。镜像卷的创建步骤如下。

（1）在动态磁盘的某个要创建镜像卷的未分配空间上右击，在弹出的快捷菜单中选择“新建卷”命令，弹出“新建卷向导”对话框。

（2）单击“下一步”按钮，在弹出的对话框中选择“镜像”单选按钮（一定要存在两个以上的动态磁盘，此选项才可选）。

（3）单击“下一步”按钮，在打开的对话框中为镜像磁盘选择磁盘，并指定磁盘空间大小。首先要确保两个动态磁盘上有足够的未分配空间，把两个镜像的磁盘都添加到对话框右边“已选的”列表框中，然后再在“选择空间量”滚动列表框中指定新建卷的磁盘空间大小。

（4）单击“下一步”按钮，在弹出的对话框中为镜像卷指定驱动器符号（从未分配的盘符中分配），注意，这时两个镜像卷使用同一个驱动器符号，当作一个驱动器使用，实际上这就是 RAID-1 磁盘阵列模式。

（5）单击“下一步”按钮，在弹出的对话框中选择要以何种格式和方式格式化镜像卷。如果磁盘完好，最好选择“执行快速格式化”复选框，进行快速格式化对磁盘的操作最少，速度也最快。

（6）单击“下一步”按钮，弹出一个向导完成对话框，在对话框中显示了前面创建新卷过程中所做的各项配置，单击“完成”按钮系统对所选卷进行格式化后即完成镜像卷的创建。

5）RAID-5 卷

RAID 通过廉价和冗余的磁盘系统，将数据写入多个廉价磁盘，从而保证单一硬盘的损坏不会导致数据的丢失。Windows Server 2003 通过给该卷的每个硬盘分区中添加奇偶校验信息带区来实现容错。如果某个硬盘出现故障，Windows Server 2003 便可以用其余硬盘上的数据和奇偶校验信息重建发生故障的硬盘上的数据。RAID-5 卷的创建步骤如下。

（1）在“磁盘管理”中，右击欲设置 RAID 的磁盘，在快捷菜单中选择“新建卷”菜单项，弹出 “欢迎使用新建卷向导”对话框。

（2）单击“下一步”按钮，在“选择卷类型”对话框中选择欲创建的 RAID-5 卷。

（3）单击“下一步”按钮，弹出“选择磁盘”对话框。在“所有可用的动态磁盘”列表框中选择欲添加的磁盘，并单击“添加”按钮，即可将其添加至该 RAID-5 卷，并显示在“选定的动态磁盘”列表框中。

（4）添加完毕（至少添加至 3 块硬盘），单击“下一步”按钮，在“指派驱动器号和路径”对话框中选中“指派驱动器号”单选按钮，并为该 RAID-5 卷指派驱动器号，便于管理和访问。

（5）单击“下一步”按钮，在“卷区格式化”对话框中选择“按下面提供的信息格式化这个卷”单选按钮，并采用默认的 NTFS 文件系统和分配单位大小。在此可以为该 RAID-5 卷指定一个卷标，用于与其他卷相区别。

（6）单击“下一步”按钮，弹出“正在完成新建卷向导”对话框，提示卷的创建即将完成；然后单击“完成”按钮，系统自动格式化新创建的卷后即完成 RAID-5 卷的创建。

3. 磁盘配额管理

1）磁盘配额

磁盘配额是基于用户和分区的文件存储管理工具。通过磁盘配额管理，网络管理员可以对本地用户或登录到本地计算机的远程用户可以使用的磁盘空间进行合理的分配，每一个用户只能使用网络管理员分配的磁盘空间，以避免对资源的滥用。

Windows Server 2003 系统的 NTFS 文件系统支持用户磁盘配额管理功能，可有效地管理用户的网络磁盘空间的使用。在启用磁盘配额功能时，管理员可设置其中的两个参数：

- 磁盘配额限度：该参数用于指定允许用户使用的最大磁盘空间容量。
- 磁盘配额警告级别：该参数指定一用户接近其配额限制的值。

启用卷的磁盘配额时，磁盘配额不会应用到现有的卷用户上，这时可以通过在“配额项目”窗口中添加新的配额项目来将磁盘空间配额应用到现有的卷用户上。由于磁盘配额能够监视单个用户卷的使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷上的其他用户的磁盘配额。在用户看来与在一个独立的磁盘卷中进行操作没什么两样。另外，要支持磁盘配额，磁盘卷必须使用 NTFS 文件系统格式化，并且不受卷中用户文件的文件夹位置的限制。

2）启用磁盘配额

启用磁盘配额，可以在用户超过管理员所指定的磁盘空间时，阻止其进一步使用磁盘空间或记录用户的使用情况。启用磁盘配额的方法如下：

（1）在 Windows 资源管理器中，右击欲启用磁盘配额的卷，在快捷菜单中选择“属性”命令，打开“磁盘属性”对话框。

（2）单击“配额”标签，切换到如图 6-35 所示的“配额”选项卡。选中“启用配额管理”复选框，其下的各个复选框将变为可用状态，其中，选择“拒绝将磁盘空间给超过配额限制的用户”复选框，表示磁盘使用空间超过配额限制的用户将收到来自 Windows 的“磁盘空间不足”的提示信息，并且在没有从中删除和移动现存文件的情况下，无法将额外的数据写入卷中。如果撤选该复选框，则用户可以超过配额限制，无限制地使用磁盘空间。

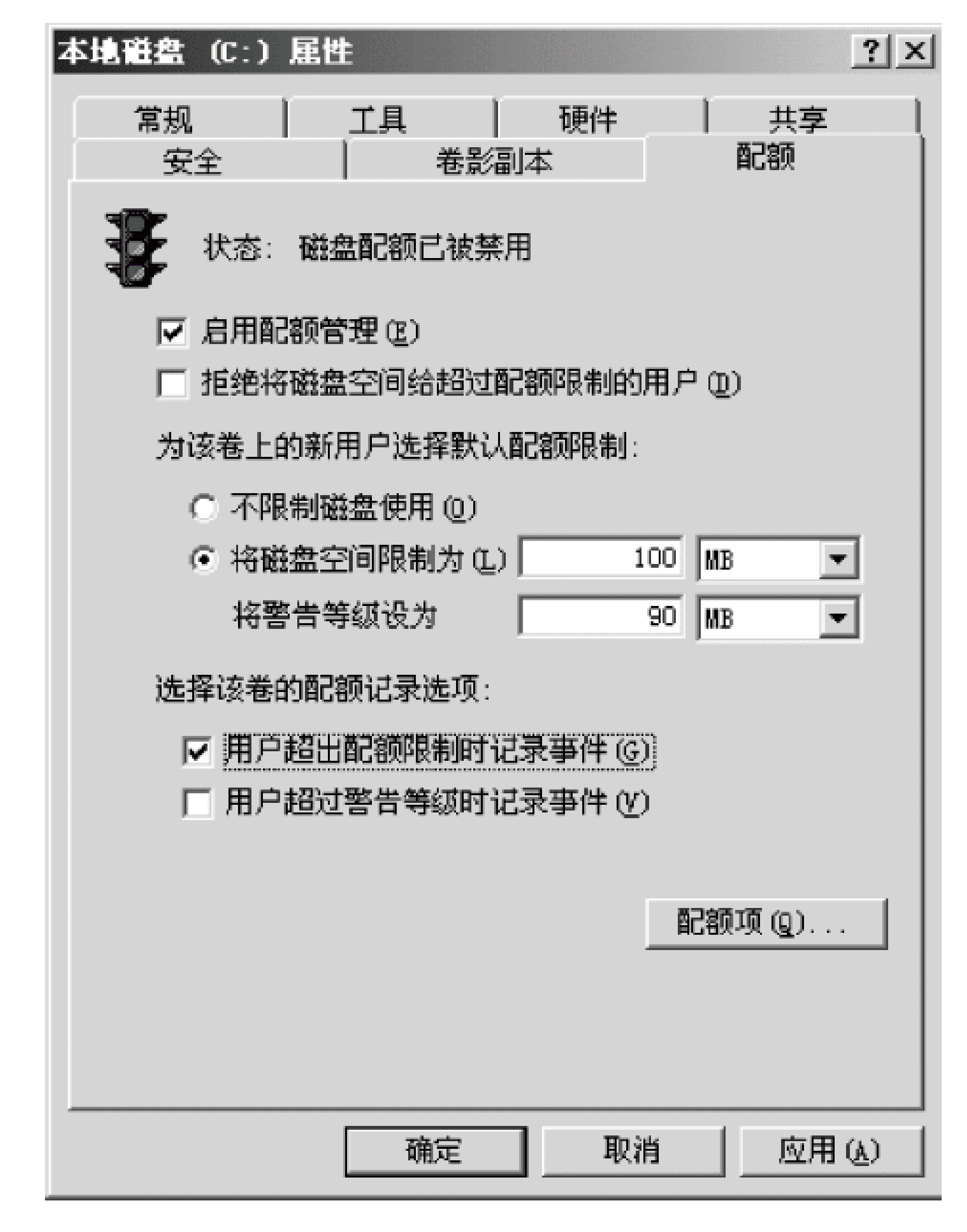


图 6-35 “配额”选项卡

（3）如果选中“不限制磁盘使用”单选按钮，则用户可以无限制地使用服务器磁盘空间。选中“将磁盘空间限制为”和“将警告等级设为”单选按钮，管理员可以输入允许卷的新用户使用的磁盘空间，在用户使用的磁盘空间接近警告值时发出警告。

（4）选中“用户超出配额限制时记录事件”复选框，如果启用磁盘配额，则只要用户超过管理员设置的配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用事件查看器，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志。

（5）选中“用户超过警告等级时记录事件”复选框，如果启用配额，则只要用户超过管理员设置的警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用事件查看器，通过筛选磁盘事件类型来查看这些事件。

（6）单击“确定”按钮，保存所做设置，启用磁盘配额。

6.4.3 逻辑资源管理

逻辑资源是指利用计算机系统通过通信设备传播和网络软件管理的各种信息资源的总和。逻辑资源的狭义理解为：信息资源就是指文献资源或者数据资源，或者各种媒介和形式的信息的集合，包括文字、音像、印刷品、电子信息、数据库等限于信息本身的资源。逻辑资源的广义理解为：信息资源是信息活动中各种要素的总称，既包含信息本身，也包含信息相关的人员、设备、技术和资金等各种资源。

本章 6.5 和 6.6 节的内容实属企业逻辑资源的管理，下面以 Windows Server 2003 的文件管理为例介绍一般逻辑资源的管理。

1. 文件管理

1）文件服务器的主要功能

在企业网络中，为了有效地执行各项文件管理功能，通常是把一台运行 Windows Server 2003 系统的成员服务器配置成“文件服务器”。文件服务器提供网络上文件所处的中心位置，可供存储文件并通过网络与用户共享文件。当用户需要重要文件时，他们可以访问文件服务器上的文件，而不必在各自独立的计算机之间传送文件。如果网络用户需要对相同文件和可通过网络访问的应用程序访问权限，就要将该计算机配置为文件服务器。默认情况下，文件服务器角色安装有下列功能。

(1) 文件服务器管理：文件服务器管理控制台为管理文件服务器提供集中的工具。使用文件服务器管理，可以创建和管理共享，设置配额限制，创建存储利用情况报告，将数据复制到文件服务器和从文件服务器中复制数据，管理存储区域网络(SAN)，以及与 UNIX 和 Macintosh 系统共享文件。

(2) 存储报告：使用存储报告，可以分析服务器上的磁盘空间是如何使用的。例如，可以生成识别重复文件的按需或计划报告，然后删除这些复制文件以便回收磁盘空间。

(3) 配额和文件屏蔽：使用配额，可以限制卷或文件夹子树大小，可以将 Windows 配置为在达到配额限制时通知用户；使用文件屏蔽，可以防止某些类型的文件被保存到文件夹或卷。文件屏蔽有助于确保用户不在服务器上保存某些可能导致用户违反知识产权法的非关键性数据和文件。

(4) DFS 管理：使用“DFS 管理”管理单元，可以管理从分支机构中的服务器到数据中心服务器的数据复制。这样，数据可以被集中备份，而不必在分支机构备份数据。使用“DFS 管理”管理单元，还可以对位于不同服务器上的共享文件夹进行分组并将其作为虚拟文件夹树(称为“名称空间”)提供给用户。名称空间可以提供很多好处，包括提高数据的可用性、分担负载和简化数据迁移。

2）配置文件服务器

文件服务是局域网中最常用的服务之一，在局域网中搭建文件服务器以后，可以通过设置用户对共享资源的访问权限来保证共享资源的安全。配置文件服务器的步骤如下：

(1) 先将计算机的文件分区格式转换成 NTFS；然后以系统管理员身份登录系统，在“开始”菜单中依次单击“管理工具”→“管理您的服务器”命令，打开“管理您的服务器”向导。在“添加角色到您的服务器”区域中单击“添加或删除角色”按钮，进入配置向导并单击“下一步”按钮。配置向导完成网络设置的检测后，如果是第一次使用该向导，则会进入“配置选

项”对话框。选中“自定义配置”单选按钮,并单击“下一步”按钮。

(2) 打开“服务器角色”对话框,在其列表框中选中“文件服务器”,并单击“下一步”按钮。

(3) 在打开的“文件服务器磁盘配额”对话框中选中“为此服务器的新用户设置默认磁盘空间配额”复选框,并根据磁盘存储空间及用户实际需要在“将磁盘空间限制为”和“将警告级别设置为”文本框中输入合适的数值。另外,选中“拒绝将磁盘空间给超过配额限制的用户”复选框,可以禁止用户在其已用磁盘空间达到限额后向服务器写入数据。单击“下一步”按钮,如图 6-36 所示。

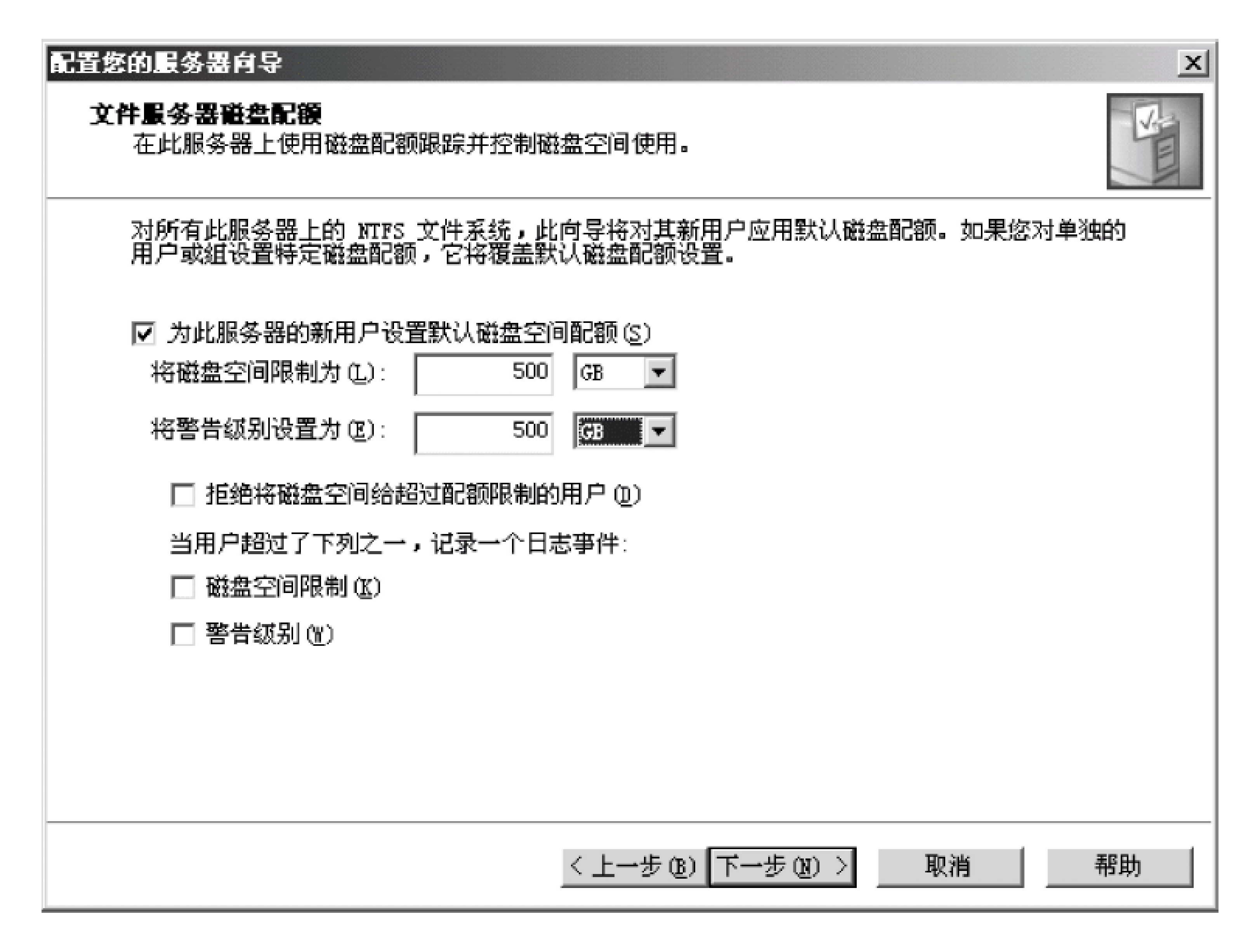


图 6-36 “文件服务器磁盘配额”对话框

(4) 在打开的“文件服务器索引服务”对话框中,选中“是,启用索引服务”单选按钮,启用对共享文件夹的索引服务。单击“下一步”按钮。

(5) 打开“选择总结”对话框,确认设置准确无误后单击“下一步”按钮。添加向导开始启用所选服务,完成后会自动打开“共享文件夹向导”对话框,然后单击“下一步”按钮。

(6) 在打开的“文件夹路径”对话框中单击“浏览”按钮,打开“浏览文件夹”对话框。在本地磁盘中找到准备设置为公共资源的文件夹,并依次单击“确定”、“下一步”按钮。

(7) 打开“名称、描述和设置”对话框,在这里可以设置共享名和描述该共享文件夹的语言,设置完毕后单击“下一步”按钮。

(8) 在打开的“权限”对话框中选中“管理员有完全访问权限;其他用户有只读访问权限”单选按钮,并依次单击“完成”按钮。

(9) 打开“共享成功”对话框,在“摘要”文本框中显示出共享文件夹路径、共享名和共享路径,其中“共享名”和“共享路径”用来向网络用户公布。单击“关闭”按钮即可完成文件服务器的建立,并可以进行相应项目的管理,如图 6-37 所示为完成后的文件服务器管理窗口。



图 6-37　文件服务器管理窗口

2. DFS 管理

分布式文件系统(Distributed File System,DFS)作为一种服务,使得系统管理员可以把局域网中不同服务器上的共享文件夹组织在一起,构建成一个目录树。这样,用户就不必知道这些共享文件夹到底在哪台服务器上,也不必一一搜索并映射它们,只需访问共享的 DFS 根目录,就能够很轻松地访问分布在网络上的文件或文件夹。

1) 分布式文件系统的类型

分布式文件系统有两种类型:一种是独立的根目录分布式文件系统,另一种是域分布式文件系统。

如图 6-38 所示是独立的根目录分布式文件系统,其目录配置信息存储在本地的主服务器上,访问根或链接的路径以主服务器名称开始,独立的根目录只有一个根目标,没有根级别的容错。因此,当根目录不可用时,整个 DFS 名称空间都不可访问。

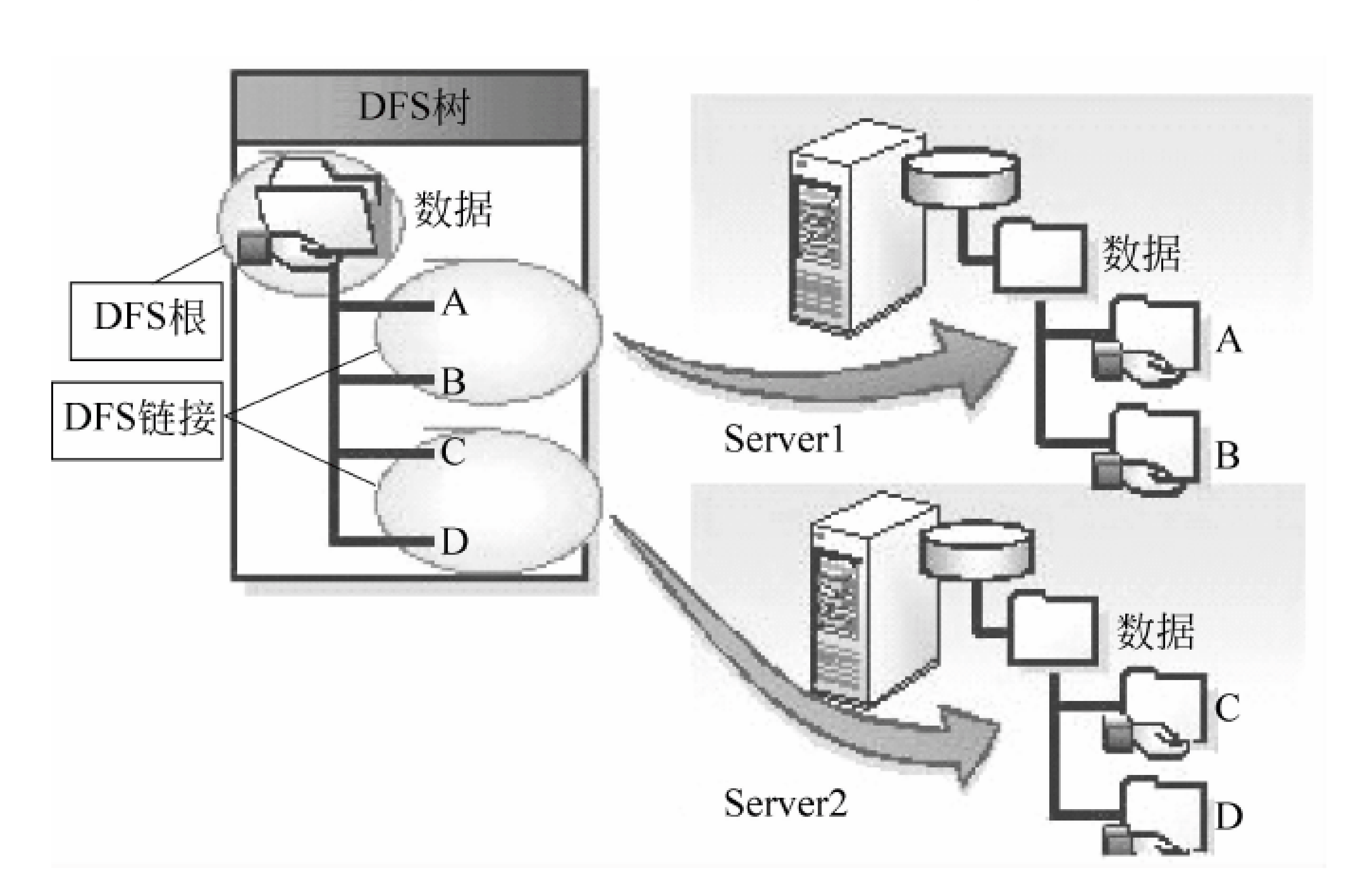


图 6-38　独立的根目录分布式文件系统示意图

独立的分布式文件系统根目录具有以下特点:

- 不使用活动目录。
- 最多只能有一个根目录级别的目标。
- 使用文件复制服务不能支持自动文件复制。

• 通过服务器群集支持容错。

如图 6-39 所示为域分布式文件系统，其中，DFS 拓扑信息被存储在活动目录中，因为该信息对域中多个域控制器都可用，所以域 DFS 为域中的所有分布式文件系统都提供了容错。

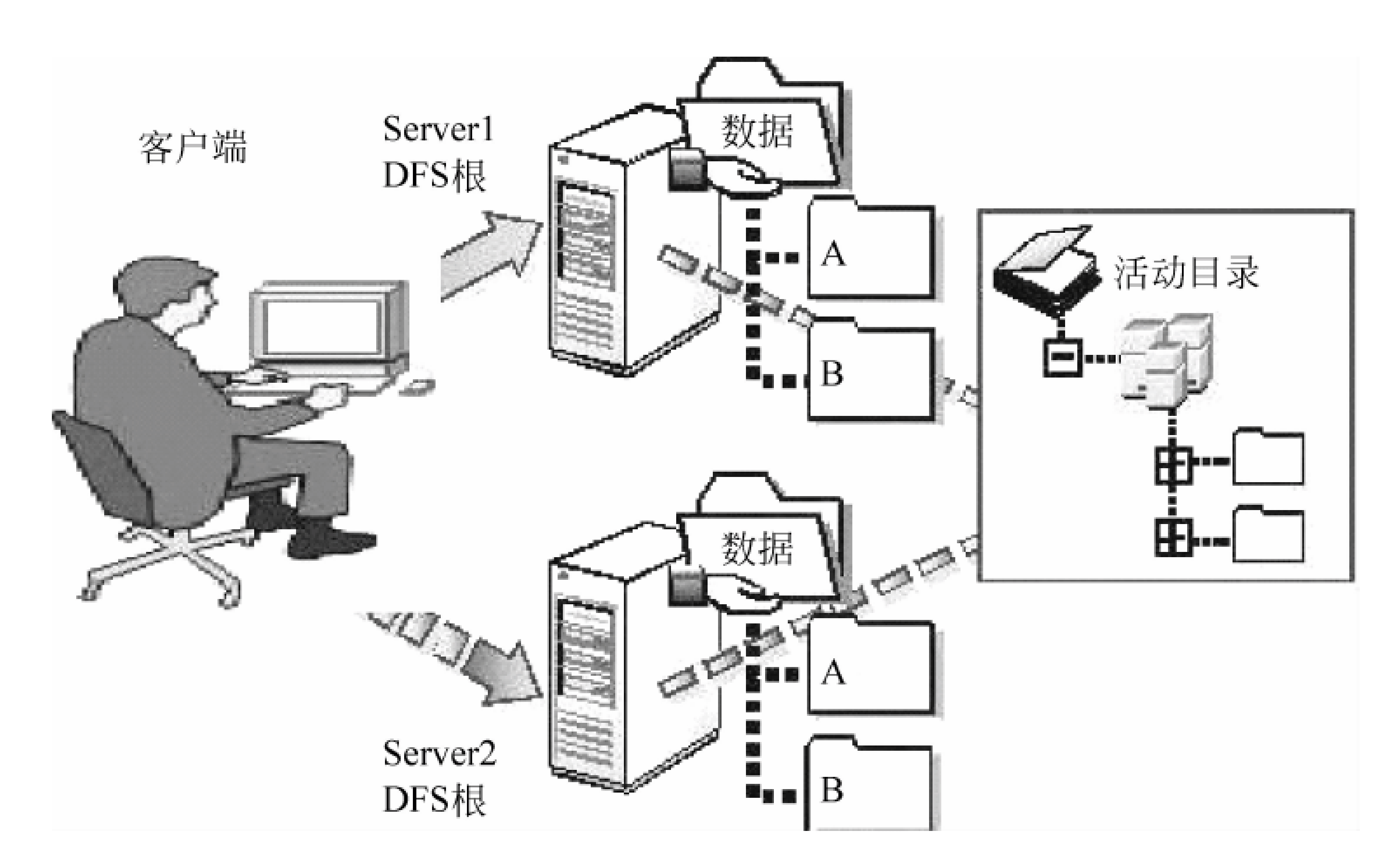


图 6-39　域分布式文件系统示意图

域 DFS 根目录具有以下特点：

• 必须在域成员服务器上创建。
• 使其 DFS 名称空间自动发布到活动目录中。
• 可以有多个根目录级别的目标。
• 通过文件复制服务支持自动文件复制。
• 通过 FRS 支持容错。

2）分布式文件系统的配置

一个完整的 DFS 需要创建 DFS 根目录、根目标（可选）、DFS 链接和 DFS 目标。

（1）创建 DFS 根目录

使用 DFS 管理工具，可以指定某个目录为 DFS 根目录。除了访问该目录外，用户还可以访问该目录的任何子文件夹，创建 DFS 根目录的步骤如下：

① 执行“开始”→“管理工具”→“分布式文件系统”菜单命令，打开如图 5-40 所示“分布式文件系统”控制台窗口。

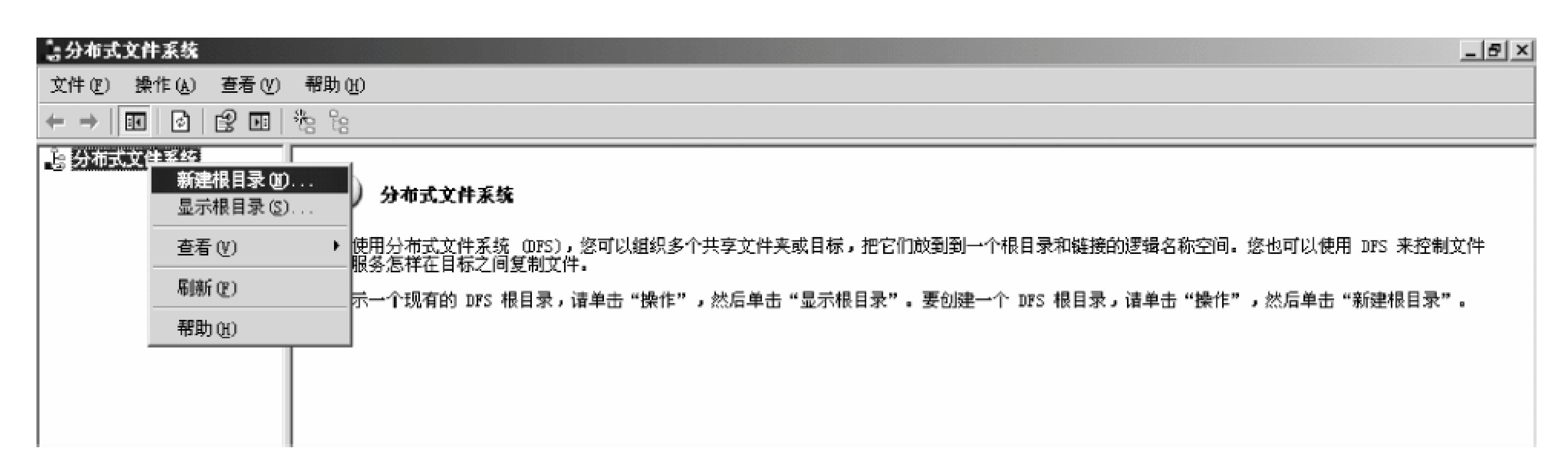


图 6-40　“分布式文件系统”控制台窗口

② 在左边导航栏中右击“分布式文件系统”命令，在弹出的快捷菜单中选择“新建根目录”命令，打开“新建根目录向导”对话框。

③ 单击“下一步”按钮，在打开的对话框中选择创建的 DFS 根目录类型，可以是域根目录，也可以是独立根目录。域根目录位于域控制器上，而独立根目录是位于成员服务器上的。在此选择“域根目录”单选按钮来创建域根目录。

④ 单击“下一步”按钮，打开如图 6-41 所示“主持域”对话框。在此对话框的“域名”文本框中输入 DFS 根目录作用的域，可以是当前域，也可以是当前域所信任的域，如子域，或者其他域树中的域。

⑤ 单击“下一步”按钮，在打开的对话框中输入 DFS 根目录所对应的主服务器名称，或单击“浏览”按钮查找相应域的主服务器。

⑥ 单击“下一步”按钮，为所创建的域根目录取一个用于识别的名称。

⑦ 单击“下一步”按钮，在打开的对话框中指定这个 DFS 根目录共享的服务器位置。

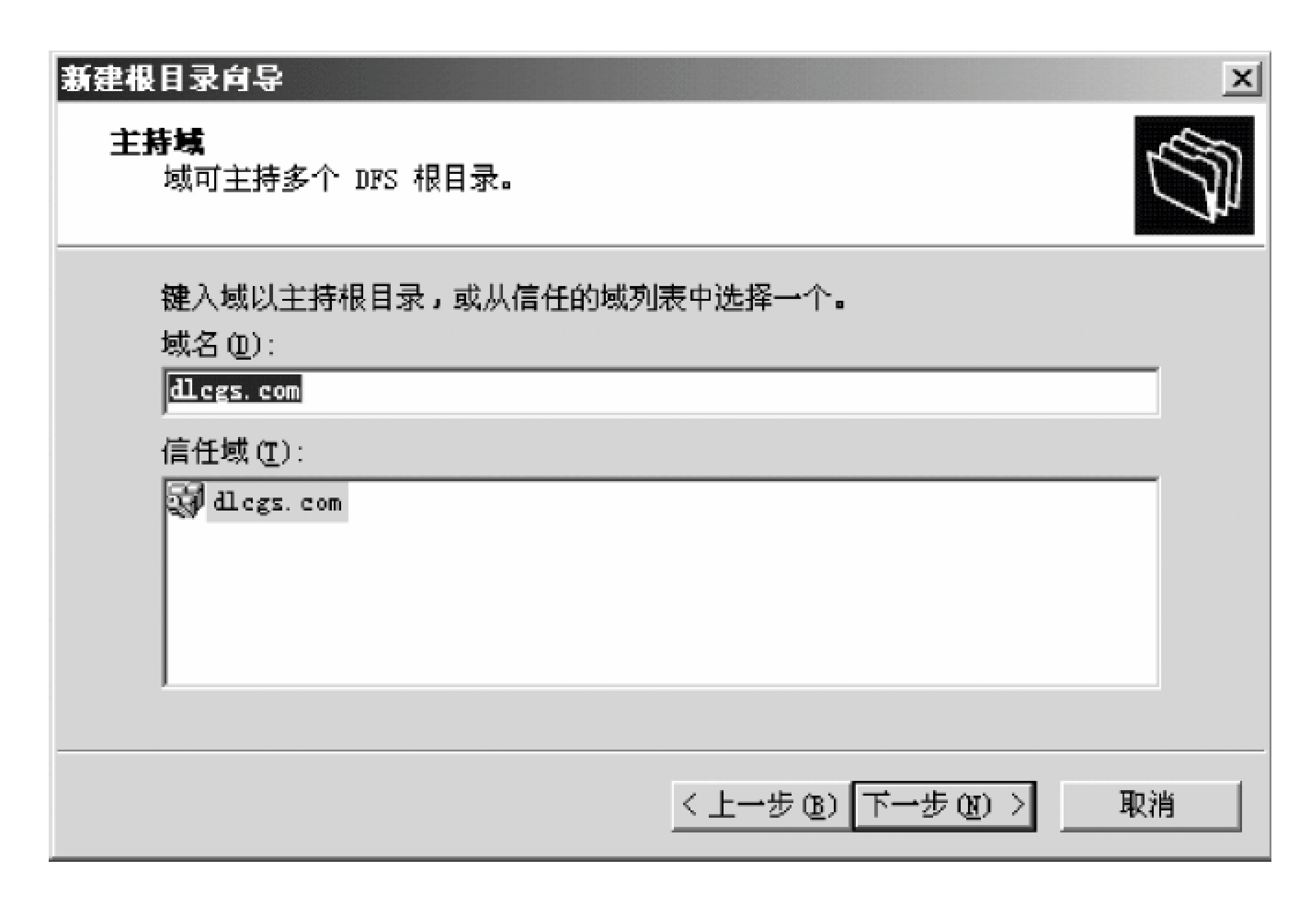


图 6-41 “主持域”对话框

⑧ 单击“下一步”按钮打开向导完成对话框，直接单击“完成”按钮完成域 DFS 根目录的创建，如图 6-42 所示。



图 6-42 域 DFS 根目录

(2) 添加 DFS 根目标(可选)

域控制器上的一个域 DFS 根目录可以对应网络中其他许多服务器上的多个根目录，这些服务器上的根目录就相当于域 DFS 根目录的目标目录(简称根目标)。创建根目标的意义主要是用来负载均衡和容错，当共享资源访问量较大时，多个根目标就可以分担根目录的负荷，而且在根目录出现故障时，根目标仍然可以为用户提供 DFS 服务。DFS 根目标的创建步骤与 DFS 根目录的创建步骤差不多，具体如下：

① 在“分布式文件系统”控制台窗口中选择相应的根目录，右击，在弹出的快捷菜单中选择“新建根目录目标”命令，在打开的对话框中选择根目标所对应的服务器。

② 正确选择了根目标所对应的服务器后，如果在所选服务器上没有创建与根目录共享文件夹名一样的共享文件夹，则在单击“下一步”按钮后，重新指定创建根目标共享文件夹的位置。

③ 配置好创建根目标共享文件夹位置后，打开向导完成对话框。直接单击“完成”按钮完成一个根目标的创建。一个 DFS 根目录可以创建多个分布于多个服务器上的 DFS 根目标，其他根目标的创建方法一样。

(3) 添加 DFS 链接

DFS 链接是 DFS 名称空间的元素，它是 DFS 系统中真正的共享资源。它们位于根目录下方并映射到 DFS 根目录，或者映射到一个或多个根目标。访问 DFS 名称空间的用户看到的是根目录下作为文件夹而列出的链接名，而不是目标的实际名称和物理位置，它们的关系实际有些像 Web 站点和 FTP 站点中的虚拟目录。由于链接名不受目标名称或位置的限制，所以可以创建对用户具有意义的链接名。

添加 DFS 链接的方法很简单，只需在“分布式文件系统”控制台窗口 DFS 根目录上右击，在弹出的快捷菜单中选择“新建链接”命令，打开如图 6-43 所示的“新建链接”对话框。在“链接名称”文本框中输入新链接的名称，在“目标路径”文本框中输入新链接的目标路径，或单击“浏览”按钮，从中选择网络中需要放入 DFS 根目录中的共享文件夹即可。

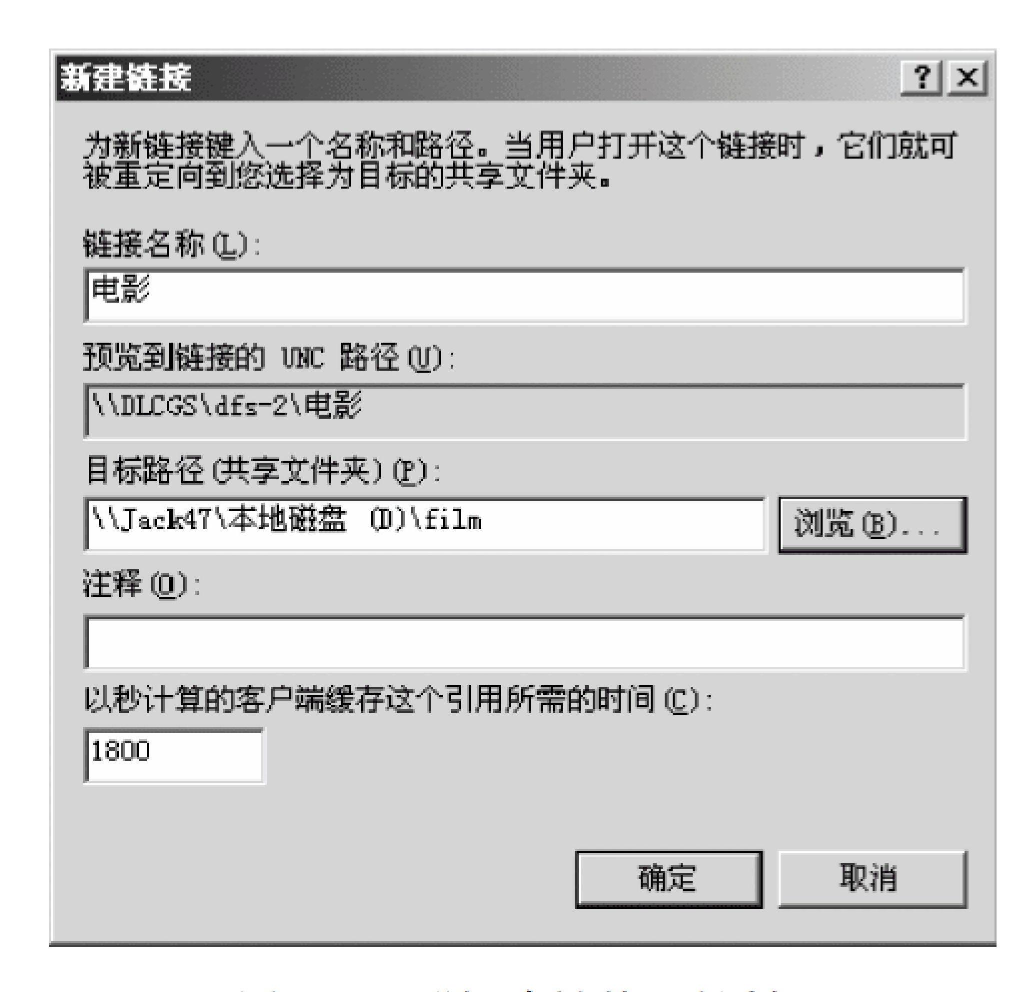


图 6-43 “新建链接”对话框

(4) 添加 DFS 目标

对于每个 DFS 链接，可以创建该 DFS 链接指向的目标集，也就是可以有多个目标。在目标集中，创建 DFS 链接时已将第一个文件夹添加到该集。使用 DFS 管理工具的“新建目标”对话框添加随后的目标。添加目标的方法如下：

① 在“分布式文件系统”控制台窗口 DFS 链接上右击，在弹出的快捷菜单中选择“新建目标”命令，在打开的对话框中指定该链接的目标的共享文件夹。如果不选择“将这个目标添加到复制集中”复选框，则直接把这个目标共享文件夹添加到 DFS 链接的目标集中。

② 如果选择了“将这个目标添加到复制集中”复选框，则会提示用户“配置复制后才能复制目标”，然后在弹出“配置复制向导”对话框中进行相应的配置即可。

③ 单击“完成”按钮完成目标创建。

通过以上 DFS 根目录、DFS 根目标、DFS 链接和 DFS 目标的创建，就完成一个完整的 DFS 系统创建，如图 6-44 所示。这样用户只需要访问根目录，或 DFS 根目标就可以访问所需要的共享文件资源，而不必到各服务器上去一一查找具体的共享文件夹。这一方面方便了用户的访问，另一方面也方便了管理员对网络中共享资源的管理。

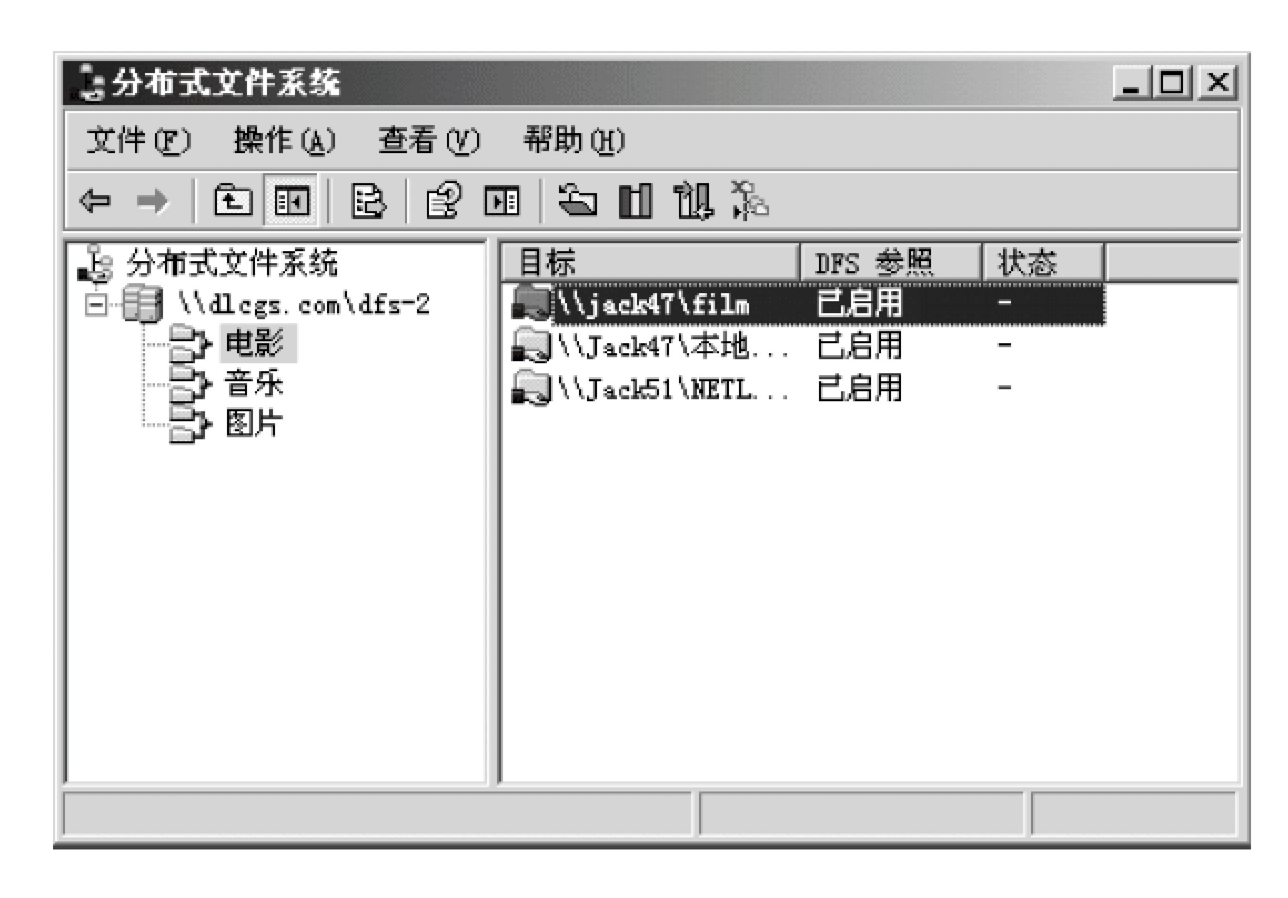


图 6-44 DFS 系统

3）DFS 的复制组

DFS 复制是一个基于状态的新型多主机复制引擎，支持复制计划和带宽限制。在一个 DFS 文件夹有多个目标的情况下，这些目标所对应的共享文件夹内的文件必须同步，可以让这些目标之间自动复制文件以使文件保持同步，不过用户需要将这些目标所在的服务器设置为同一个复制组，并做必要的设置。创建复制组步骤如下：

（1）单击“开始”按钮，指向“管理工具”，然后单击“DFS 管理”。

（2）在控制台树中，右击“复制”节点，然后从快捷菜单中选择“新建复制组”命令。

（3）按照“新建复制组向导”中的指示完成其他操作。

6.5 业务管理

网络管理员除了掌握必要的软件和硬件技术以外，还需要对企业生产和经营的业务应用系统，如财务管理系统、办公自动化系统、ERP 系统等的基本知识有深刻的理解，并掌握其基本操作。这不但能够保障网络基础设施正常、稳定地运行，而且还能够确保生产、经营业务的正常开展。

6.5.1 电子政务管理

1. 电子政务

电子政务是政府在其管理和服务职能中运用现代信息和通信技术，实现政府组织结构和工作流程的重组优化，超越时间和空间，以及部门分割的制约，全方位地向社会提供优质、规范、透明的服务。

一般而言，政府的主要职能在于经济管理、市场监管、社会管理和公共服务。而电子政

务就是要将这四大职能电子化、网络化，利用现代信息技术对政府进行信息化改造，以提高政府部门依法行政的水平。电子政务应用主要包括政府与政府、政府与企业、政府与公民之间3方面。

1）政府间的电子政务

政府间的电子政务是上下级政府、不同地方政府、不同政府部门之间的电子政务，主要包括以下内容。

（1）电子法规政策系统：对所有政府部门和工作人员提供相关的现行有效的各项法律、法规、规章、行政命令和政策规范，使所有政府机关和工作人员真正做到有法可依，有法必依。

（2）电子公文系统：在保证信息安全的前提下，在政府上下级、部门之间传送有关的政府公文，如报告、请示、批复、公告、通知、通报等，使政务信息十分快捷地在政府间和政府内流转，提高政府公文处理速度。

（3）电子司法档案系统：在政府司法机关之间共享司法信息（如公安机关的刑事犯罪记录、审判机关的审判案例、检察机关检察案例等），可以改善司法工作效率，提高司法人员综合能力。

（4）电子财政管理系统：向各级国家权力机关、审计部门和相关机构提供分级、分部门历年的政府财政预算及其执行情况，包括从明细到汇总的财政收入、开支、拨付款数据以及相关的文字说明和图表，便于有关领导和部门及时掌握和监控财政状况。

（5）电子办公系统：通过网络完成机关工作人员的诸多事务性的工作，节约时间和费用，提高工作效率，如工作人员通过网络申请出差、请假、文件复制、使用办公设施和设备、下载政府机关经常使用的各种表格，报销出差费用等。

（6）电子培训系统：对政府工作人员提供各种综合性和专业性的网络教育课程，特别是适应信息时代对政府的要求，加强对员工与信息技术有关的专业培训，员工可以通过网络随时随地注册参加培训课程、接受培训、参加考试等。

（7）业绩评价系统：按照设定的任务目标、工作标准和完成情况，对政府各部门业绩进行科学的测量和评估。

2）政府对企业的电子政务

政府对企业的电子政务是指政府通过电子网络系统进行电子采购与招标，精简管理业务流程，快捷迅速地为企业提供各种信息服务，主要包括以下内容。

（1）电子采购与招标：通过网络公布政府采购与招标信息，为企业特别是中小企业参与政府采购提供必要的帮助，向他们提供政府采购的有关政策和程序，使政府采购成为阳光作业，减少徇私舞弊和暗箱操作，降低企业的交易成本，节约政府采购支出。

（2）电子税务：使企业通过政府税务网络系统，在家里或企业办公室就能完成税务登记、税务申报、税款划拨、查询税收公报、了解税收政策等业务，既方便了企业，也减少了政府的开支。

（3）电子证照办理：让企业通过Internet申请办理各种证件和执照，缩短办证周期，减轻企业负担，如企业营业执照的申请、受理、审核、发放、年检、登记项目变更、核销，统计证、土地和房产证、建筑许可证、环境评估报告等证件、执照和审批事项的办理。

（4）信息咨询服务：政府将拥有的各种数据库信息对企业开放，方便企业利用。如法

律法规规章政策数据库、政府经济白皮书、国际贸易统计资料等信息。

(5) 中小企业电子服务：政府利用宏观管理优势和集合优势，为提高中小企业国际竞争力和知名度提供各种帮助。包括为中小企业提供统一政府网站入口，帮助中小企业同电子商务供应商争取有利的能够负担的电子商务应用解决方案等。

3) 政府对公民的电子政务

政府对公民的电子政务是指政府通过网络系统为公民提供的各种服务，主要包括以下内容。

(1) 教育培训服务：建立全国性的教育平台，并资助所有的学校和图书馆接入互联网和政府教育平台；政府出资购买教育资源，然后对学校和学生提供；重点加强对信息技术能力的教育和培训，以适应信息时代的挑战。

(2) 就业服务：通过电话、Internet 或其他媒体向公民提供工作机会和就业培训，促进就业。如开设网上人才市场或劳动市场，提供与就业有关的工作职位缺口数据库和求职数据库信息；在就业管理和劳动部门所在地或其他公共场所建立网站入口，为没有计算机的公民提供接入 Internet 寻找工作职位的机会；为求职者提供网上就业培训，分析就业形势，指导就业方向。

(3) 电子医疗服务：通过政府网站提供医疗保险政策信息、医药信息，执业医生信息，为公民提供全面的医疗服务，公民可通过网络查询自己的医疗保险个人账户余额和当地公共医疗账户的情况；查询国家新审批的药品的成分、功效、试验数据、使用方法及其他详细数据，提高自我保健的能力；查询当地医院的级别和执业医生的资格情况，选择合适的医生和医院。

(4) 社会保险网络服务：通过电子网络建立覆盖地区甚至国家的社会保险网络，使公民通过网络及时全面地了解自己的养老、失业、工伤、医疗等社会保险账户的明细情况，有利于加深社会保障体系的建立和普及；通过网络公布最低收入家庭补助，增加透明度；还可以通过网络直接办理有关的社会保险理赔手续。

(5) 公民信息服务：使公民得以方便、容易、费用低廉地接入政府法律法规规章数据库；通过网络提供被选举人背景资料，促进公民对被选举人的了解；通过在线评论和意见反馈了解公民对政府工作的意见，改进政府工作。

(6) 交通管理服务：通过建立电子交通网站提供对交通工具和司机的管理与服务。

(7) 公民电子税务：允许公民个人通过电子报税系统申报个人所得税、财产税等个人税务。

(8) 电子证件服务：允许居民通过网络办理结婚证、离婚证、出生证、死亡证明等有关证书。

2. 电子政务系统

电子政务系统是面向政府机关内部、其他政府机构、企业、社会公众的基于互联网技术的信息处理系统，主要通过机关内部处理流程模拟、协作、信息发布，以及受理各类申请、投诉、建议、要求来实现，既有信息的发布和接收，也有交互式的处理。如图 6-45 所示为北京电子政务系统“首都之窗”的“办事服务”页面，电子政务系统是一种复杂的综合信息管理系统，通常包括以下功能。

1) 网络应用平台子系统

主要为政府内部网建设一个先进的、标准的、安全的网络运行平台，以保证整个网络系



图 6-45　北京市政务门户网站

统的基本服务完整性以及系统的开放性与可伸缩性。该子系统是内网用户进入的入口，可对用户身份进行认证，为用户提供基本的网络服务功能以及各种专业网络服务的通道。该子系统可提供以下功能。

(1) 用户登录认证：确定用户身份，一经认证，全网通用，根据用户身份和权限提供相应的网络服务。

(2) 用户密码修改：用户可随时更改自己的密码，系统能够防止密码被盗用。

(3) 电子新闻：可动态播放政府机构内部或外部的新闻事件，并进行即时加载。

(4) 电子公告：及时提供各种公告和通知。

(5) 电子论坛：提供各种专题，供用户参加讨论和发表意见。

2) 网络安全管理子系统

对政府内部网所有用户和所有网上业务系统进行统一管理，对网上的每一个用户进行授权，并对入网的每一项服务项目进行分发授权，以保证整个网络的安全运行。该子系统可提供以下功能。

(1) 人员管理：部门内的所有员工都是网上用户，系统可将每个用户看成一个独立的对象，为每个用户建立一个数字身份证，其基础数据将随着用户身份的变化而改变。

(2) 服务项目管理：对于政府内部不同的业务会有不同的管理信息系统，这些系统可称为服务项目或网上服务资源，该模块可对全网内的服务资源进行统一管理，提供对服务项目的增、删、改、存等功能。

(3) 授权配置管理：可根据用户的工作岗位和责任，为其分配相应的网络使用资源，并

根据用户地位的变化调整授权管理，包括对所有权限进行增、删、改、存等操作。

(4) 系统维护管理：包括用户组管理、权限类型管理、管理员账号口令管理、系统访问日志管理、公共信息维护管理等。

3) 信息发布子系统

信息发布子系统为用户提供了一个统一的信息共享环境，无论共享信息在物理上如何分布，都可使用户及时方便地获取信息。政府部门可根据自身的业务特点，将在业务运转过程中产生的共享信息在网上实时发布。该子系统还提供各类业务系统上网发布接口，以及信息发布模板和工具，使普通用户不需要编程就可建立信息发布栏目，并可自行对栏目信息进行编辑与维护。该子系统可提供以下功能。

(1) 政务信息发布：在政府部门的日常工作中，经常要印刷大量内部刊物，如调研报告、内部参考、专题研究等，该功能可将这些信息有序地发布到网上去，并提供信息的查询、编辑、修改等维护功能。

(2) 领导日程安排：政府机关的领导工作繁忙，活动较多，建立网上领导日程安排可加强沟通，提高工作效率，便于整个部门统筹安排工作。

(3) 会议安排：提供会议日程、会议地点、会议纪要、与会人员等信息的发布和维护功能。

(4) 共享业务信息：在政府网上会同时有多种业务系统运行，每种业务处理系统的使用部门和人员都互不相同。信息发布子系统可为每个业务系统提供共享信息的发布标准和发布结构，用户只要有权限，就可通过发布系统查看到各种业务系统共享出来的信息。

4) 公文流转子系统

公文流转子系统为政府部门或企业集团创建了一个协同办公的网络环境，使各种业务处理工作可完全在网络环境下完成，有效地提高了办公效率，增强了决策制定的可协调性。该子系统可提供以下功能。

(1) 新业务启动：每个政府业务的运转可作为一个工作流程，当用户在网上进行协同工作时，可根据业务需求来确定已有工作流程中的一个，启动后即可在网上进行传递和流转。典型的业务工作流程有收文流程、发文流程、签报流程、出差流程、协同阅稿流程等。

(2) 任务管理：当政府内部网进入正常运转时，网上会同时进行多种业务流程，某个用户可能有多个业务处理请示或指示，这种业务工作就是“任务”。任务管理模块可提供任务接收、任务处理、任务发送、任务传递等功能。

(3) 文件录入与修改：在公文流转子系统执行之前，政府部门历史上已经人工积累了大量文件数据。为了使用户能够及时、准确地进行网络查询，该模块提供了历史文件录入、文件查询权限的设置、必填项目的检验等功能。

(4) 文件归档与查询：在每个工作流程结束后，所有文件信息都自动归档，同时可对已归档的文件进行查询，包括对任意字段的查询、对正文的全文检索等功能。

5) 经济计划管理子系统

经济计划管理子系统可为综合管理部门提供便利的计划编制工具，以提高制订计划的效率和能力。每个计划是一个集合，包括多个分类计划本，如农业计划、社会发展计划等。每个计划本由多张计划表格组成，计划表格则由各种计划指标构成。因此，计划的基础就是计划指标数据库。计划编制人员可把计划表格制成模板，将每个单元格与数据库指标建立

关联。在制订新一年的计划编制时，可将上一年的计划作为模板直接导入，通过调整基准年度产生当年的计划草稿，在此基础之上，可方便地制作各种计划。该子系统可提供以下功能。

(1) 计划结构维护：计划由计划本、计划表格和计划指标集构成，计划结构维护就是对构成计划的各个部分进行维护，包括对计划本身、计划本、计划表格、计划文字等进行增、删、改、存和排序等功能。

(2) 数据维护：选择指标值的时间、地区、类别、数值等属性后，用户可直接输入新值，系统本身具有校验功能。

(3) 计划查询：包括对计划结构、指标值、计划表格、计划文字等内容的查询。

(4) 计划表格制作：用户在 Excel 中画出计划表格清样后，系统可在表格元素与指标对象数据之间建立对应关系。

6) 项目管理子系统

项目管理子系统可为政府部门的项目管理业务提供管理软件，动态跟踪项目的全过程，为政府决策提供依据。传统的项目管理是直接根据项目的业务需求来定制的，一旦项目属性发生变化，项目管理软件就需要重新改造。该子系统则以政府投资项目为设计对象，把各种项目信息作为项目属性，其中有些项目属性为系统默认属性(如项目名称、单位等)，有些项目属性则为用户自定义属性，使用户可在系统原型基础上再确定特有属性，并对项目进行编辑与维护。此外，用户查询到某个项目后，就相当于打开了该项目的主页，与该项目相关的所有信息都有相应的连接，使对项目的跟踪、查询更加方便快捷。该子系统可提供以下功能。

(1) 项目属性维护：系统为用户提供了项目的基本属性，用户通过使用这些属性可完成基本的项目管理工作。如果用户有特殊需求，还可使用项目属性维护功能进行扩展，并对项目属性的数据字典进行维护，包括对项目建设的性质、目的、类型、水平、资金来源、审批级别等内容的维护。

(2) 项目数据编辑：在项目属性维护完成之后，确定了项目结构，用户可对项目的数据内容进行增、删、改、查、存和排序处理。

(3) 项目分析：用户可对所有项目进行多种角度的分析，包括对项目分布、项目结构、项目效益、项目水平等在线分析，并能生成各种分析统计报表。

(4) 项目跟踪：每个项目都有一个主页系统，用户可通过浏览或条件查询得到项目列表，并进入项目主页，了解和查看项目主页上的相关信息，包括项目基本情况、项目背景、各阶段进展情况、相关项目对比、项目预期效益、资金到位情况、项目建设中的问题、项目负责单位的更换及原因等内容。

3. 电子政务系统管理

1) 电子政务业务系统

电子政务的业务系统主要为公务员和领导提供办公和决策方面的支持。主要功能包括行政办公管理、人力资源管理、财政财务管理、决策支持、知识管理等。电子政务环境下的行政办公管理实现内部行政沟通、协调和监控，提高办公信息流转，提高办公自动化程度。电子政务环境下的人力资源管理，对政府内部的人力资源情况有一个全面的了解和管理，做到人尽其才。电子政务环境下的财政财务管理，通过先进的信息化手段对政府和事业单位的日常支出进行管理。电子政务环境下的决策支持，提供在线决策支持能力，帮助政府提高决策的科学性和规范性，全面提升政府办公效率。电子政务环境下的知识管理，力图能够将最

恰当的知识在最恰当的时间传递给最恰当的人,以便使他们采取最恰当的行动,做出最好的决策,避免重复错误和重复工作。

以 SmartGov 电子政务业务系统为例,其功能如图 6-46 所示。



图 6-46　SmartGov 子系统

SmartGov 的后台管理页面如图 6-47 所示。



图 6-47　SmartGov 的后台管理页面

2）电子政务系统的管理

网络管理员对电子政务系统的日常管理主要包括以下几方面。

(1) 网上信息发布管理：对现有的政府主页进行重新设计和构建,使其能为辖区内的法人单位、公众获取政府信息并直接在网上接受政府提供的各种服务提供一个统一的网络平台。

(2) 办公自动化管理：办公自动化不是简单地把传统的办公模式照搬到网上，而是要作业务部门的重组和业务流程的优化，网络管理员应该超越技术的范畴，能够有参与办公自动化业务流程的制定和规范的能力。

(3) 网上交互式办公管理：用网络信息安全技术作为保证，确保7天×24小时电子政务的实现。虽然各个部门的业务是相对独立的，但当用户办理一件事时还是要求与多个部门依次打交道，网络管理员应能够保证交互式办公活动的正常开展。

(4) 资源共享与协同工作管理：在各个部门信息资源共享的基础上实现多个部门网上联合办公。网络管理员应该确保政府信息资源可以供全社会安全共享，以推动社会经济的发展。

6.5.2 电子商务管理

1. 电子商务管理的概念

电子商务管理是指为实现企业战略目标对电子商务应用中的技术和商业及其创新活动进行计划、组织、领导和控制的过程；是开展电子商务活动的各类企业在新的技术环境下，如何借助互联网技术，开展采购、生产、营销以及与之相关的财务、人员、信息等经营活动，实现其商业目标。

2. 电子商务管理的内容

电子商务管理主要包括与从事电子商务活动的组织有关的人、财、物、时间、信息、技术、环境、客户等要素系统组成的信息流、资金流、物流的资源管理等内容，涉及以下几方面。

(1) 电子商务经营战略：主要包括电子商务经营战略分析、电子商务经营战略环境、电子商务经营战略目标、电子商务经营战略方法等内容。

(2) 电子商务资源管理：主要包括电子商务人力资源管理的含义、电子商务人力资源的构成、电子商务人力资源管理实践、电子商务人力资源管理制度、电子商务物力资源管理、电子商务无形资产管理、电子商务运营资本含义与特征、企业资本运营原则与方式、企业资本运营案例分析等内容。

(3) 电子商务信息流管理：主要包括企业信息化的含义、企业信息化过程、企业信息化目标、信息源的概念、信息源的属性、信息源的类型、信息搜集与处理、信息存储与检索、企业电子商务信息流、企业电子商务信息流管理系统、企业电子商务信息管理系统运行等内容。

(4) 电子商务物流管理：主要包括物流的内容及其地位作用、第三方物流、企业自营物流、企业物流运作方式、企业物流运作内容与原则、企业物流运作理念与目标、企业物流运作的主要方法等内容。

(5) 电子商务资金流管理：主要包括企业资金流的构成、网络经济对资金流管理的影响、企业资金流管理体系建设、现代资金流管理系统的发展、MRP11 系统的资金流管理、ERP 系统的资金管理等内容。

3. 电子商务管理系统

电子商务管理系统是对企业的电子商务活动进行管理的软件系统。以动易 BizIdea 产品为例，BizIdea 整合了电子商务的全部业务流程，实现了全程式电子商务管理。BizIdea 提供了与多种企业 ERP 系统的对接接口及系列对接功能(如供应商管理、订货单管理、退货单管理等)，可供企业将自身 B2C 电子商务平台与内部 ERP 系统进行全面整合及对接，以达到双方的数据互通和协同管理。此外，BizIdea 还将提供基于企业内部管理的任务管理系

统，可供企业内部对员工工作计划及工作任务进行统一而有序的管理，以加强企业内部工作效率管理。

BizIdea是新一代企业电子商务管理系统，是一套专门面向大中型企业级电子商务平台构建与管理的解决方案，拥有全套的企业电子商务支持工具。从站点构建到商品陈列、库存管理，从订单协同处理到在线支付和客户关系管理，从促销导购到销售分析财务管理等辅助决策工具，从站内资讯内容管理到人才招聘在线支持等。尤为适用于各类进行直销/分销电子商务运营的传统生产企业和作为企业分销渠道的销售/贸易型企业。其电子商务管理系统的功能包括图6-48所示的子系统。



图6-48　BizIdea子系统

BizIdea企业版后台管理页面如图6-49所示。



图6-49　BizIdea企业版后台管理页面

6.5.3 企业管理系统

企业管理系统工程是目前信息技术中的一个大类。它以企业管理需求为基础，以信息技术为支撑，为企业提供数据信息的综合管理办法，包括 ERP、CRM、HR、PM、KM、OA 等内容。目前常用的业务管理软件有 SAP、用友、金蝶、速达、管家婆等。

企业管理系统能够帮助企业实现办公自动化、程序化，能够对信息进行集中管理，一般管理软件都是进销存、财务、ERP 等模式。高级的企业管理软件是企业咨询顾问形式的企业管理软件，包括工作分析、绩效考核、薪酬设计、招聘系统、员工培训、生涯规划的制度与方法，能激活企业内在的运营能力，达到利润倍增等效果。下面将简单介绍可以在网上直接体验的两款软件。

1. “企管家”软件

“企管家”是 B/S 和 C/S 双模式的面向服务的业务、生产、财务等企业管理软件系列，能全面满足企业对总部、工厂、分店、分支、仓库等分散部门实时的统一的管理要求。企业人员不管身在何地，都可以随时联网工作，业务数据能够实时汇总分析，从而确保管理层及时洞察经营问题，抓住稍纵即逝的业务机会。

“企管家”的主页面如图 6-50 所示，包括我的工作、基本设置、业务系统、账务管理、生产系统、系统设置和相关链接模块。详细功能和具体操作读者可登录网站 http://www.easy-erp.com:6666/免费体验。



图 6-50 “企管家”主页面

“企管家”系统实现的主要功能如下。

(1) 采购：先付款再收货、先收货再付款、采购退货、估价入库、采购费用分配等多种采购业务处理。

(2) 销售：先收款再发货、先发货再收款、分期收款、销售退货、销售费用计入成本等多种业务处理。

(3) 库存：盘点、报损报溢、调拨、调量、调价、组装拆卸等多种库存变动处理方法。

(4) 提供加权平均、个别计价和先进先出等 4 种存货核算方法，能准确进行成本核算。

(5) 动态管理应收、应付账款，方便准确冲转各种往来账，可及时掌握往来总账及明细账目。

(6) 库存统计、流量分析、销售分析、采购分析、业绩分析、年度分析等各种分析报表，方便决策。

（7）生产：任务、领料、验收等多种业务处理，自动生成物料需求表。

2. 速用企业管理系列软件

速用企业管理系列软件包括采购管理、销售管理、财务管理和仓库管理等系列功能，读者可登录网站 http://www.superuse.com.cn/Product.html 免费下载试用。速用进销存软件（企业进销存管理、财务管理一体化解决方案）的导航页面如图 6-51 所示。



图 6-51　速用进销存软件导航页面

（1）销售管理

销售管理是对产品或商品销售过程的管理，包括销售报价、销售订货、仓库发货、销售退货、销售发票处理、客户服务管理、价格及折扣管理、订单管理、销售统计报表、销售分析、信用管理等功能。销售管理模块的功能是管理客户档案、销售线索、销售活动、业务报告、统计销售业绩，适合企业销售部门办公和管理使用，协助销售人员快速管理客户、销售和业务的重要数据。销售管理的功能如图 6-52 所示。



图 6-52　销售管理功能

（2）采购管理

采购管理是从计划下达、采购单生成、采购单执行、到货接收、检验入库、采购发票的收集到采购结算的采购活动的全过程，对采购过程中物流运动的各个环节状态进行严密的跟踪、监督，实现对企业采购活动执行过程的科学管理。采购管理包括采购计划、订单管理及发票校验三个组件。采购管理的功能如图 6-53 所示。



图 6-53　采购管理功能

（3）财务管理

财务管理是在一定的整体目标下，关于资产的购置（投资）、资本的融通（筹资）和经营中现金流量（营运资金），以及利润分配的管理。财务管理是企业管理的一个组成部分，它是根据财经法规制度，按照财务管理的原则，组织企业财务活动，处理财务关系的一项经济管理工作。财务管理的功能如图 6-54 所示。

（4）仓库管理

仓库管理也叫仓储管理，指的是对仓储货物的收发、结存等活动的有效控制，其目的是保证企业仓储货物的完好无损，确保生产经营活动的正常进行，并在此基础上对各类货物的变动状况进行分类记录，以明确的图表方式表达仓储货物在数量、品质方面的状况，以及目前所在的地理位置、部门、订单归属和仓储分散程度等情况的综合管理形式。仓库管理的功能如图 6-55 所示。

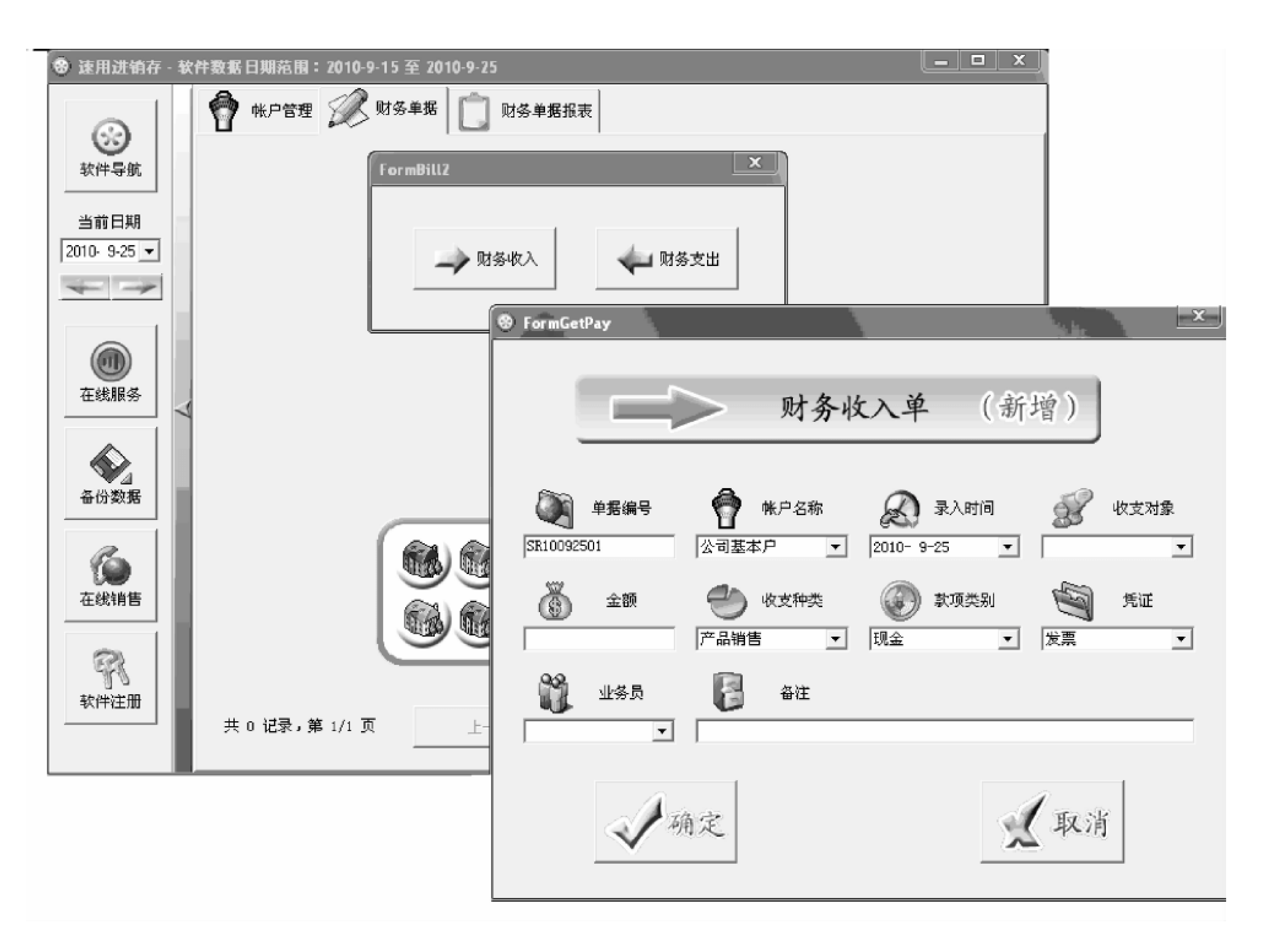


图 6-54　财务管理功能

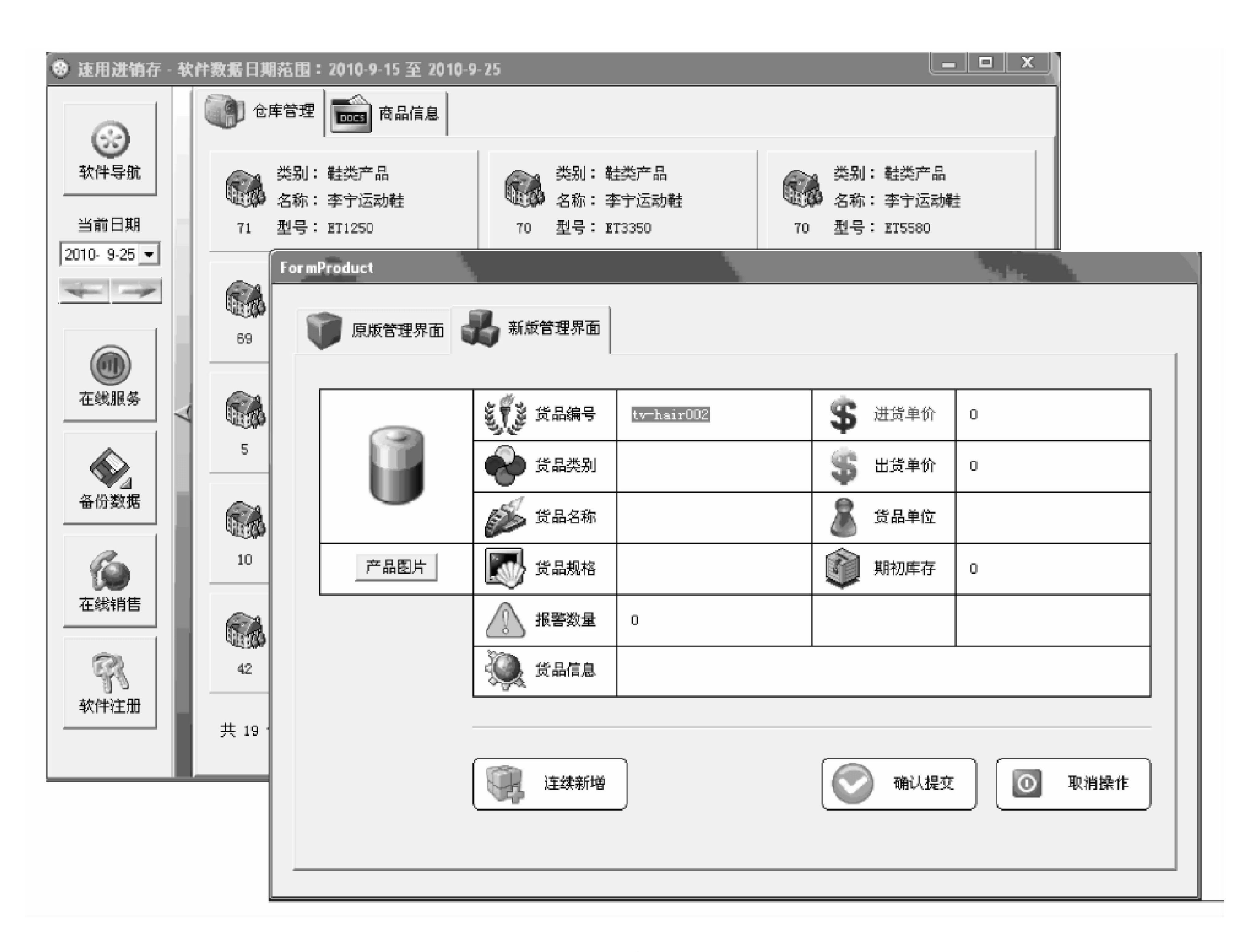


图 6-55　仓库管理功能

6.6 文档管理

6.6.1 文档管理的概念

“文档”一词原指那些在计算机中创建的电子文档或扫描成数字格式的文档，现在文档的意义已经得到扩展，还包括电子邮件、传真、即时信息、PowerPoint 演示、WIKI 和多媒体等形式。文档是信息资源，文档管理是企业生产、技术、科研和经营等活动的真实记录和基础性工作。

文档作为与企业同步发展的无形资产，在企业管理等各方面正积极地发挥应有的重要作用。所以，规范化、科学化的文档管理是企业必须做好的一项重要工作。建立一套适应本企业业务特点、体现企业规范化、科学管理水平的文档体系，将为企业各项综合业务、研究工作的开展创造必要条件，对规避和抵御各种风险起到一定作用。

6.6.2 企业文档管理系统

企业文档管理系统应用程序可以用来创建一个企业所有文件的单一视图，并提供工作流工具，以监测和控制修改，从而使文件检索更容易。在这样的系统中，所有格式的文件都要被标注和索引，这一点很重要。因为这样它们才能通过关键字或全文搜索快速地被找到。

基于 Web 平台的网络办公系统通常采用 B/S 架构设计，将应用服务集中于统一的应用服务器之中。用户无论身处世界哪个地方，只要可以访问 Internet，就可以完成企业的日常业务，真正步入分散经营、集中控制的商务管理模式。

文档管理系统是现代网络办公系统的一部分，它融合了当前最流行的管理思想，即对工作流、信息流和知识管理的规范管理和增值利用，为用户提供了一个先进、高效的信息化工作平台。文档管理系统将人从繁琐、无序、低端的工作中解放出来处理更有价值、更重要的事务，整体提高了企业办事效率和对信息的可控性，使企业管理趋于完善，提高执行力，最终实现单位市场竞争力全面提升的目标。文档管理系统主要有以下作用。

1. 整合企业资源

(1) 通过网络技术将企业的人力资源、客户资源、知识资源、经验资源、硬件资源、制度资源、文化资源等集成在一个平台上进行管理使用。

(2) 资源整合，实现各种资源的互相促进和增值，创造企业发展的最优环境，促进企业发展。

(3) 对人力资源、客户资源实现更加有效的控制和管理，保持稳定的工作团队和客户关系。

(4) 有效积累企业优秀员工的知识、技能、经验、心得并向所有员工开放，使员工互相学习，快速提高业务水平，达到事半功倍的效果。

(5) 将企业的产品、各种办公用品等硬件资源进行分类管理，更加方便、可靠、透明，发挥它们最大的功效。

(6) 建立正规、科学、开放的企业的制度和文化，保持企业旺盛的生命力，保证企业健康持续发展。

2. 加快信息流通

(1) 下达的文件、通知、任务可以在几秒钟内同时传达到相关人员,无任何中间环节。

(2) 员工的意见和建议都可以畅通无阻地直接反馈到最高领导层,便于及时发现问题、改进过程和发现人才。

(3) 即使是在外地的员工或分支机构也可以实时保持和企业的沟通,保持紧密的联系。

(4) 所有员工都可以在第一时间知道企业的最新动态和决策,更加关注企业的发展。

(5) 所有员工都能及时了解企业产品的库存、价格、销量等信息,及时调整工作。

(6) 下属可以在第一时间将工作进度和市场信息反映给上级领导,使企业以快制胜。

(7) 员工们能够在网上轻松、直接、公平地发言、交流,建立融洽的团队关系和企业文化。

3. 规范办公流程

(1) 建立起一个紧密、协调、可靠、简单的管理机制,让企业充满活力,促进企业持续发展。

(2) 使员工责任明确,权限分明,具体事务落实到人,查有所依,杜绝推脱、扯皮现象。

(3) 企业的办公流程变得规范、有序,效率大大提高,执行力大大提高。

(4) 彻底消除信息传递中的阻塞、延误、失真,保证正确、及时的反应。

(5) 领导层可以清晰、准确地了解员工对某一事件的倾向性以做出正确的决策。

(6) 离职员工无法带走自己的客户资源,避免人员流动给企业带来的客户流失的风险。

(7) 通过网络而不是麻烦的电话来询问项目进度,从而节省大量时间、精力和电话费。

(8) 领导层可以及时关注下属的工作动态,及时发现问题,不会因为疏漏而丢掉重要的订单或客户。

(9) 员工们每天都记录下当天的工作内容和心得,领导层可以直接查看、指导。

(10) 企业可以免去诸如打印、分发、打电话、找人等诸多困扰,节约纸张、人力等办公成本,能够将资源和精力、时间用于核心业务上。

(11) 员工间、员工与领导之间可以方便、直接、充分地进行交流,通过正确的手段而不是凭个人交际能力来沟通。

4. 提高办事效率

(1) 有效协调多部门之间的协同工作问题,实现高效协作办公。

(2) 信息流通速度成倍提高,带来员工反应速度的成倍提高。

(3) 可以快捷地同时给大量客户发送手机短信,保持密切、融洽、稳定的客户关系。

(4) 领导层能够方便地随时查看分配过的任务数量、领取人及其进度情况,跟踪监督以提高执行效率和执行力度。

(5) 员工能够清晰地查看到自己当前领取的各项任务状态以合理安排时间。

(6) 员工之间可以快捷地在线发送文件、通知和留言,不必打电话甚至亲自到处找人,时时沟通,节省时间,提高效率。

(7) 消除打印、复印、分发等诸多中间环节,沟通点对点,传递一指通。

(8) 随时随地都能够在网上快捷地查看各种资料,并能调阅和打印出来,省去了为看一份文件而到处寻找浪费掉的大量时间。

6.6.3 企业文档管理系统的使用

以绿叶 OA 办公系统(http://www.oa169.com)为例,其主页面如图 6-56 所示,主要包括办公桌面、部门主页、文件传输、发送消息、手机短信、资源共享、内部论坛、通信录、系统集成和视频演示等常用功能。

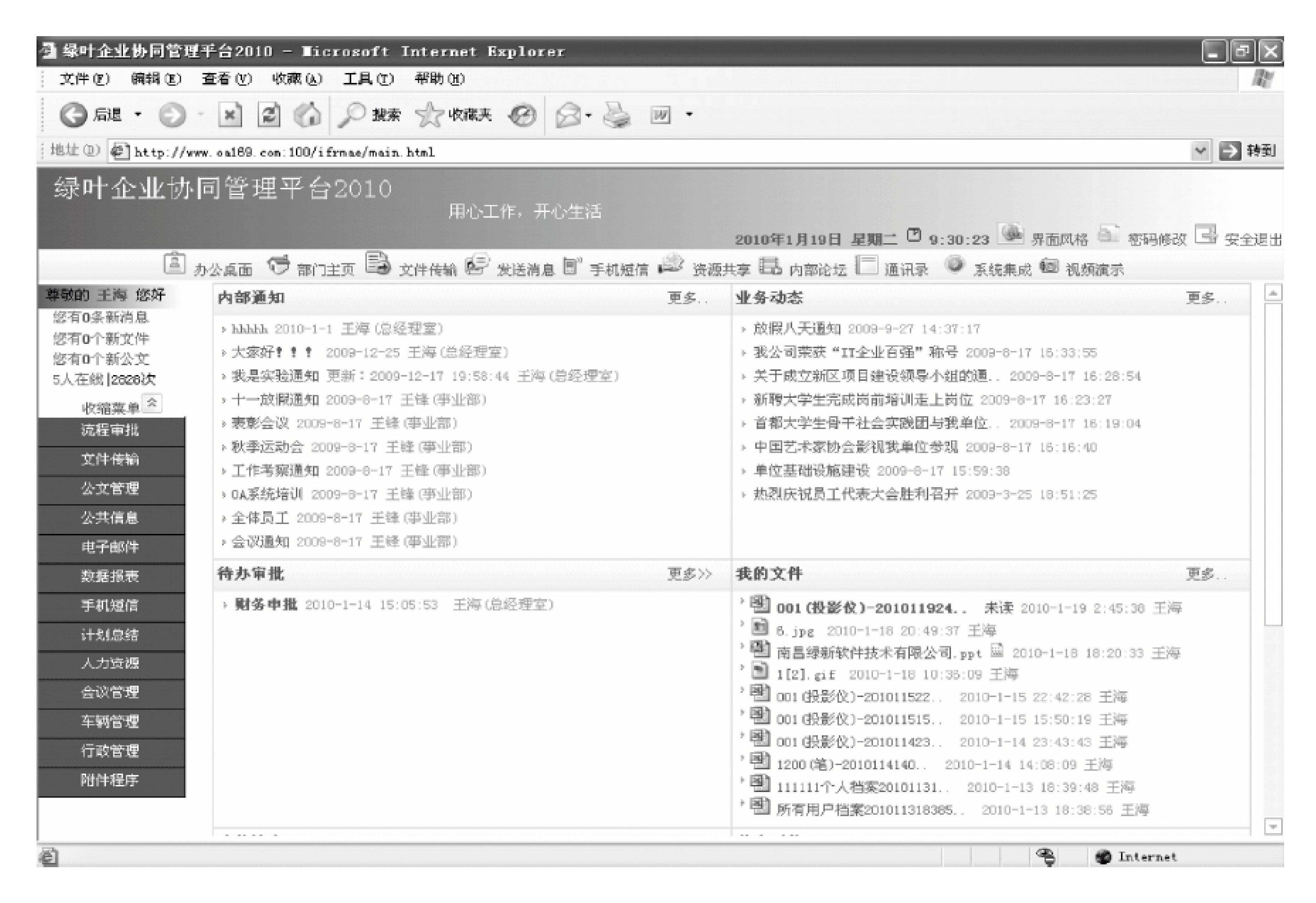


图 6-56　绿叶 OA 办公系统主页面

详细功能和操作如左侧导航栏所示,主要包括流程审批、文件传输、公文管理、公共信息、电子邮件、数据报表、手机短信、计划总结、工作总结、人力资源、会议管理、车辆管理、行政管理和附件程序。下面简单介绍几个功能。

1. 流程审批

工作流程审批系统采用可视化、组件化、向导式、节点式流程配置引擎,支持电子签名、手机提醒,方便企业快速扩展新的业务功能和模块,适应业务的灵活多样化需求,满足大中型集团企业内部流程的建立、监控、变更等要求,实现工作流程的自动化、标准化和规范化。

(1) 发起流程,可新建自由流程与固定流程:

- 自由流程:可自由设定流转路径、内容、表单附件等。
- 固定流程:按照已设定的流程路径与表单进行流转,并可按照流程基础设置参数。

(2) 流程审批:按照流水号、流程标题、状态、当前流转、审批人数、发送人等主要信息读取所有接收流程审批信息,对未读流程加粗显示,使审批用户对流程概况有最基本了解。进入流程审批,提交审批结果与内容,流程将进入下一流程节点用户。同时,提交审批结果、编辑批注流程表单附件,可发送消息与手机短信提醒发起人与下一审批人;支持流程删除、查询、催办管理,支持附件收藏、转发、下载等,支持流程表单附件的电子签名、手写批注、电子印章、痕迹保留、防止文档篡改、U 盾签名安全应用。

(3) 流程监控管理:按照流水号、流程标题、状态、当前流转、审批人数等主要信息读取

所有已发送流程审批信息，对流程审批人未读流程加粗显示。可修改流程标题、内容、表单附件，增加与删除表单附件；修改流转顺序，强制设定某节点为当前流转或终止当前流转，可增加与删除节点，完成委托、转办等任务指令。同时，支持流程删除与查询。支持流程表单附件的电子签名、手写批注、电子印章、痕迹保留、防止文档篡改、U盾签名安全应用。支持流程设计图形显示管理。

（4）权限与其他：流程发起、审批、监控管理、模板、类别、选项等操作可由管理员在后台进行授权管理。类别设置管理可以根据单位实际情况建立流程模板类别，包括行政、人事、财务、营销等。选项设置中的“节点审批后，该节点是否可修改审批结果与内容”决定在用户提交审批结果后是否可进行审批结果修改；“发起固定流程，是否可以管理内容与表单附件”决定设置发起固定流程时，是否可以修改即将发起流程的内容或者添加或修改表单附件，最大程度地满足用户对流程模板的需要。

2. 文件传输

（1）文件传输：支持点对点、点对多集群批量高速传输大小文件，提供直接传输给自己的方式；支持发送文件的同时增加文件备注说明与整合短信系统的功能，支持文件回执与小秘书提醒服务。

（2）文件传输记录：报告文件是否阅读，记录接收人阅读下载记录，包括时间、IP等信息；支持已发文件下载与继续发送，追踪已发文件接收对象的所有回复，提供对已发文件进行备注说明的功能。

（3）文件接收：进入文件接收系统，可对文件进行在线阅读、下载、转发、回复、删除等，对来自集群接收的文件，系统会自动显示接收对象，以提醒用户可区别性转发文件，避免重复发送。支持对接收文件进行按照部门分类与自助类别管理与分类，便于查阅与管理；支持已发送文件和接收文件查询检索服务。此外，对接收到的文件提供即时提醒，包括语音、文字、小窗口、短消息提醒等功能。主页面如图6-57所示。



图 6-57　文件接收页面

3. 公文管理

(1) 公文发送：公文审批支持流程自定义，支持一对一、一对多个人与部门发送及群发公文，支持 Word、Excel、PowerPoint、WPS 文件可编辑人员选择与批量大文件上传、手机短信提醒的功能。

(2) 公文接收：可在线阅读、下载公文附件与公文部门分类，可进行意见批注与提供痕迹保留、电子印章、键盘批注，保护文档不被篡改；可对签阅意见进行修改与删除，实时查看公文批示意见。公文整合短信系统，提供公文回执与小秘书即时提醒服务与公文催办。支持接收公文查询功能。

(3) 公文发送记录：发送人可查看与删除发送记录，系统自动对公文阅读下载状况进行统计，包括阅读人姓名、部门、时间、IP 等，编辑修改 Word、Excel、PowerPoint、WPS 公文；支持已发公文查询功能。

4. 公共信息

公共信息功能提供企业内部信息共享上传下载通道，用户可对需要共享的文件、图片、动画、视频、音乐等按照类别进行快速上传，管理员可在后台进行类别管理，建立一套单位内部共享体系。同时支持分布式跨服务器跨站点数据文件共享。进入共享区后可在线浏览与下载文件，并支持收藏与转发。支持实时共享开关、删除等。同时提供共享文件的快速分类与查询服务。其中，共享下载的页面如图 6-58 所示。



图 6-58 共享下载页面

5. 电子邮件

电子邮件功能包括内外网邮件、手机 WAP 邮件服务。内网邮件与短信系统集成，外网邮件支持 Internet 邮件发送、接收、回复等。用户与管理员可自由配置邮件 SMTP 与 POP3 信息，用户个人配置信息将只对其个人收发邮件产生作用，管理员进行的邮件配置将对全局用户产生效力，但与用户个人的邮件配置同步存在与互相保护。系统内置 WAP 手机邮件程序，可在 IIS 中配置 WAP 服务器(无须通信服务商提供支持)，系统将自动接收到来自手

机传输的邮件数据。

6. 手机短信

手机短信功能支持移动、联通、小灵通短信收发，主要实现形式包括短信发送与群发，系统各种消息短信提醒与信息回执，密码与手机绑定，手机信息可存储于 OA 数据库中。系统记录每条短信发送状态，返回短信服务器物理发送信息，便于追踪、查看短信发送质量与效果，后台管理员可实时管理短信账户、短信数据管理、查询等。基于组件技术，无须硬件 Modem 设备与联系通信服务商，只需进行账户充值使用。可应用于商业信息发布、客户关系管理、呼叫中心、订票与信息查询、移动办公、短信互动平台等。

7. 计划总结

计划总结功能支持在线撰写工作计划，提供浏览、修改、删除、实时开关等管理操作。按照权限不同，上级部门可浏览下属工作总结，并提供工作计划列表与数据分类查询服务。其中“日程安排”页面如图 6-59 所示。



图 6-59 日程安排页面

8. 工作总结

工作总结功能支持月总结、季度总结、年度总结。表单项目包括月份、季度、年度工作，常规工作，下一步工作计划，创新、问题反馈、意见与建议。可实现浏览、修改、删除、开关等操作。按照权限不同，上级部门可浏览下属工作总结，提供按年、月、季度、部门综合查询数据与部门工作总结分类。

9. 人力资源

人力资源功能主要包括人事档案管理与查询、简历合同附件上传、照片管理、权限分配、数据导出、打印等功能。同时可对用户简历、合同、电子照片进行实时更新、下载、转发、收藏，支持多幅照片上传与存储应用。其中“请假管理”页面如图 6-60 所示。





图 6-60 “请假管理”页面

6.7 本章小结

本章主要介绍了日常运维与管理的知识和操作，重点应理解和掌握日常网络、业务运维与管理的理论基础和基本操作的方法和技能。

本章首先介绍了企业网站的特点以及后台管理的基本操作；然后介绍了网络布线的基本知识和布线子系统设计与施工的技术与管理；接着介绍了 SQL 数据库的管理、物理及逻辑资源管理，以及业务管理的知识和基本操作方法；最后介绍了企业文档管理系统。

作为网络管理员，除了掌握网络管理的技术以外，还要理解和掌握企事业单位的基本业务，业务管理是网络管理的重要组成部分。对大中型企业来说，基本网络管理系统与综合业务管理系统的有机结合是至关重要的。

习　题　6

一、选择题

1. 一个完整的企业网站，无论多么复杂或多么简单，都含有 4 个要素，下列选项中哪个不属于企业网站的要素(　　)。

A. 结构　　B. 内容　　C. 服务　　D. 信息

2. SQL Server 代理服务由(　　)3 个部分组成。

A. 管理者　　B. 作业　　C. 警报　　D. 操作员

3. 电子政务应用主要包括(　　)之间 3 个方面。

A. 政府与政府　　B. 政府与企业　　C. 政府与公民　　D. 政府与军队

4. 企业管理系统能够帮助企业实现办公自动化、程序化，以及对信息集中管理。一般管理软件都是(　　)、ERP 等模式。

A. 进销存　　B. 财务　　C. 统计　　D. 分析

二、简答题

1. 企业网站的特征是什么?
2. 简述企业网站的功能。
3. 影响企业网站可信度的因素有哪些?
4. 简述网站管理的内容。
5. 在综合布线系统中如何计算配件和电缆的长度?
6. 网络工程验收的项目有哪些?
7. 网络物理资源和逻辑资源包括哪些内容?
8. 电子政务管理、电子商务管理、企业管理的内容分别是什么?

第7章 信息安全管理

7.1 信息安全管理概述

7.1.1 信息安全的概念

1. 信息安全

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能够连续、可靠、正常地运行，信息服务不中断。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。

2. 安全威胁的类型和来源

安全威胁是指对信息安全的一种潜在的侵害，威胁的实施称为攻击。一般认为，目前网络信息安全面临的威胁主要表现在信息泄露、拒绝服务、信息破坏三大类。

(1) 信息泄露：指敏感数据在有意或无意中被泄露出去或丢失，它通常包括信息在传输中丢失或泄露、信息在存储介质中丢失或泄漏、通过建立隐蔽隧道等窃取敏感信息等。

(2) 信息破坏：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

(3) 拒绝服务：不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序，使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

信息安全的威胁可能来自各个方面，影响、危害网络信息安全的因素分为自然因素和人为两类。

(1) 自然因素包括：①各种自然灾害，如水、火、雷、电、风暴、烟尘、虫害、鼠害、海啸和地震等；②系统的环境和场地条件，如温度、湿度、电源、地线和其他防护设施不良造成的威胁；③电磁辐射和电磁干扰的威胁；④硬件设备自然老化；⑤可靠性下降的威胁等。

(2) 人为因素又有无意和故意之分。无目的事件包括操作失误、意外损失、编程缺陷、意外丢失、管理不善、无意破坏等；人为故意的破坏包括敌对势力、各种计算机犯罪等。

3. 信息安全的特征

根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽

视的国家安全战略。信息安全的主要特征如下。

- 保密性：保证信息只让合法用户访问，信息系统不被非授权使用，信息不泄露给非授权的个人和实体。
- 完整性：保障信息及其处理方法的准确性、完全性；信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。信息完整性是网络信息安全的基本要求，破坏信息的完整性是影响网络信息安全的常用手段。
- 可用性：保证合法用户在需要时可以访问到信息及相关资源，计算机系统可被合法用户访问并按要求的特性使用，即当需要时能存取所需信息。

信息安全可通过一套包括政策、行为规范、流程、组织结构和软件等管制手段，来确保具体安全目标的实现。

7.1.2 信息系统安全管理的概念

1. 信息系统安全管理

信息系统安全管理是一个过程，用于维持信息系统的机密性、完整性、可用性在一个适当的、可接受的水平。信息系统安全管理是对一个信息系统的生命周期全过程实施符合安全等级责任要求的科学管理，它包括落实安全组织及安全管理人员，明确角色与职责，制定安全规划，开发安全策略，实施风险管理，制定业务持续性计划和灾难恢复计划，选择与实施安全措施，保证配置、变更的正确与安全，进行安全审计，保证维护支持，监控、检查、处理安全事件，安全意识与安全教育，人员安全管理等。

2. 信息安全管理的目标

- 真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。
- 保密性：保证机密信息不被窃听，或窃听者不能了解被窃信息的真实含义。
- 完整性：保证数据的一致性，防止数据被非法用户篡改。
- 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。
- 不可抵赖性：建立有效的责任机制，防止用户否认其行为。
- 可控制性：对信息的传播及内容具有控制能力。
- 可审查性：对出现的网络安全问题提供调查的依据和手段。

3. 信息安全管理的重要性

信息和信息支持程序、系统及网络是重要的经营资源。信息的保密性、完整性和可得性对维持企业的竞争优势、现金流动、赢利性、合法性和商业形象至关重要。

但目前的企业及其信息系统和网络正面临着来自各方面的越来越多的安全威胁，企业在安全威胁面前也越来越脆弱，许多信息系统本身的设计也不安全，通过技术手段达到的安全是很有限的，因此信息安全管理具有特别重要的意义。

一切的安全问题，归根结底是管理的问题。管理问题主要表现在两个方面：一是领导者不重视，二是员工缺乏安全意识。领导者不重视的原因，可能是因为对信息安全的认识不足，没有认真考虑过一旦出了重大信息安全事故，会给企业造成多么惨重的损失；或有些企业的领导者对信息安全管理这类没有明显效益的投资不感兴趣。如果企业的领导者都不重视信息安全问题，那么讨论信息安全管理就变得毫无意义了。企业对员工缺乏足够的、持续的信息安全教育和培训，导致员工没有足够的安全意识，带来的危害是巨大的，如果企业的

员工普遍缺乏安全意识，只凭网络管理员、信息安全管理员，企业信息安全的获得根本是不现实的。

4. 安全措施

1）计算机网络安全措施

计算机网络安全措施主要包括保护网络安全、保护应用安全和保护系统安全三个方面。

（1）保护网络安全

网络安全是为了保护应用各方网络终端系统之间通信过程的安全性。保证机密性、完整性、认证性和访问控制性是网络安全的重要因素。保护网络安全的主要措施如下：

- 全面规划网络平台的安全策略。
- 制定网络安全的管理措施。
- 使用防火墙等访问控制措施。
- 尽可能记录网络上的一切活动。
- 注意对网络设备的物理保护。
- 检验网络平台系统的脆弱性。
- 建立可靠的识别和鉴别机制。

（2）保护应用安全

保护应用安全，主要是针对特定应用所建立的安全防护措施，它独立于网络的任何其他安全防护措施。虽然有些防护措施可能是网络安全业务的一种替代或重叠，如 Web 浏览器和 Web 服务器在应用层上对网络支付结算信息包的加密都通过 IP 层加密，但是许多应用还有自己的特定安全要求。

虽然网络层上的安全仍有其特定地位，但是人们不能完全依靠它来解决业务应用的安全性。由于业务应用中的应用层对安全的要求最严格、最复杂，因此更倾向于在应用层而不是在网络层采取各种安全措施。应用层上的安全业务可以涉及认证、访问控制、机密性、数据完整性、不可否认性、Web 安全性、EDI 和网络支付等应用的安全性。

（3）保护系统安全

保护系统安全，是指从整体电子商务系统或网络支付系统的角度进行安全防护，它与网络系统硬件平台、操作系统、各种应用软件等互相关联，涉及网络支付结算的系统安全，包含下述一些措施：

- 在安装的软件中，检查和确认未知的安全漏洞。
- 技术与管理相结合，使系统具有最小穿透风险性。
- 建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

2）商务交易安全措施

商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，重点关注如何保障电子商务过程的顺利进行。各种商务交易安全服务都是通过安全技术来实现的，主要包括加密技术、认证技术和电子商务安全协议等。

（1）加密技术

加密技术是电子商务采取的基本安全措施，交易双方可根据需要在信息交换阶段使用。加密技术分为两类，即对称加密和非对称加密。

对称加密又称私钥加密，即信息的发送方和接收方用同一个密钥去加密和解密数据。

它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。如果通信双方能够确保密钥交换的安全性，那么就可以使用这种加密方法。

非对称加密又称公钥加密，使用一对密钥来分别完成加密和解密操作，其中一个公开发布(即公钥)，另一个由用户自己秘密保存(即私钥)。信息交换的过程是：甲方生成一对密钥并将其中的一把作为公钥向其他交易方公开，得到该公钥的乙方使用该密钥对信息进行加密后再发送给甲方，甲方再用自己保存的私钥对加密信息进行解密。

(2) 认证技术

认证技术是用电子手段证明发送者和接收者的身份及其文件完整性的技术，即确认双方的身份信息在传送或存储过程中未被篡改。目前常用的认证技术有数字签名和数字证书两种。

数字签名能起到电子文件认证、核准和生效的作用。如图 7-1 所示，其实现方式是把散列函数(Hash 函数)和公钥加密算法结合起来，发送方从报文文本中生成一个散列值(数字摘要)，并用自己的私钥对这个散列值进行加密，形成发送方的数字签名；然后，将这个数字签名作为报文的附件和报文一起发送给报文的接收方；报文的接收方首先从接收到的原始报文中计算出散列值，接着再用发送方的公钥来对报文附加的数字签名进行解密；如果这两个散列值相同，那么接收方就能确认该数字签名是发送方的。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充、篡改等问题。

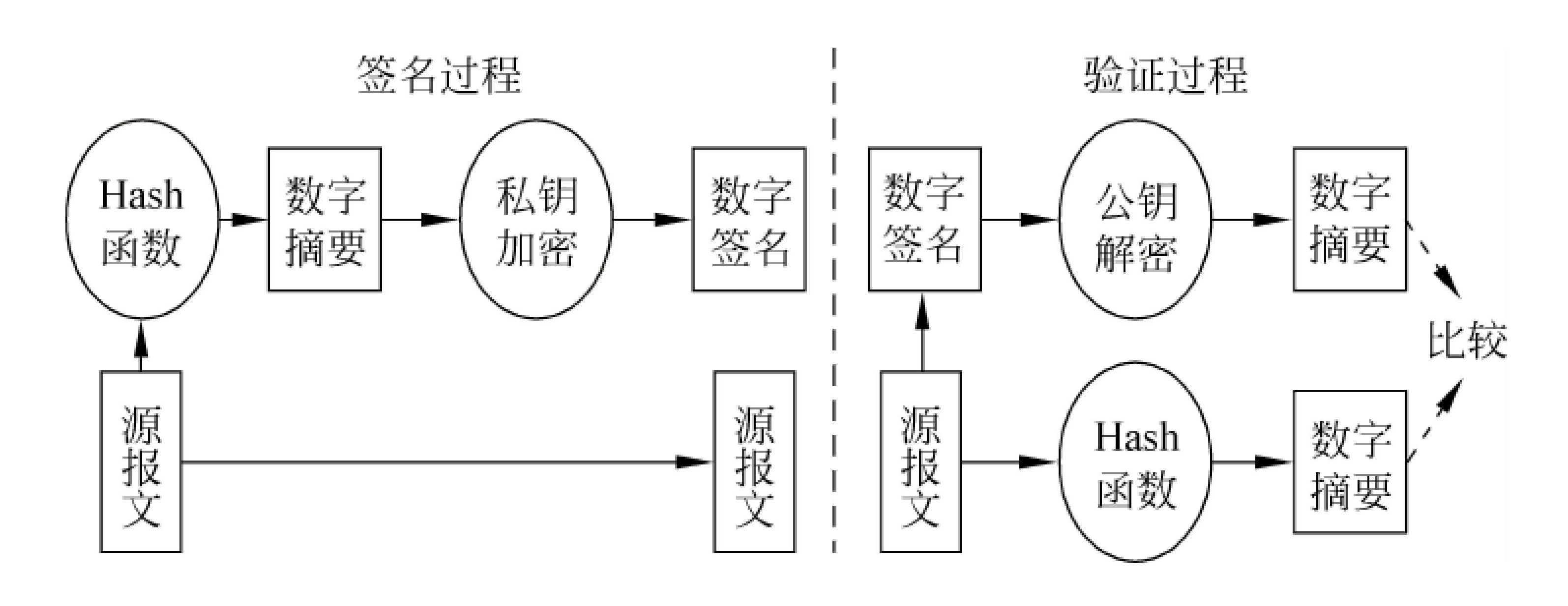


图 7-1 数字签名的原理

数字证书是一个经证书授权中心数字签名的包含公钥拥有者信息以及公钥的文件。数字证书的主要构成包括一个用户公钥、密钥所有者的身份标识符，以及被信任的第三方签名，第三方一般是用户信任的证书权威机构(Certificate Authority，CA)。用户以安全的方式向公钥证书权威机构提交他的公钥并得到证书，然后用户就可以公开这个证书。任何需要用户公钥的人都可以得到此证书，并通过相关的信任签名来验证公钥的有效性。数字证书通过标志交易各方身份信息的一系列数据，提供了一种验证各自身份的方式，用户可以用它来识别对方的身份。

(3) 电子商务安全协议

电子商务的运行还有一套完整的安全协议，目前，比较成熟的协议有 SET、SSL 等。

安全电子交易协议(Secure Electronic Transaction，SET)是专为电子商务系统设计的，它位于应用层，其认证体系十分完善，能实现多方认证。在 SET 的实现中，消费者账户信息对商家来说是保密的，但是 SET 协议十分复杂，交易数据需进行多次验证，用到多个密钥以及多次加密解密，而且在 SET 协议中除消费者与商家外，还有发卡银行、收单银行、认证中

心、支付网关等其他介入者,如图 7-2 所示为 SET 交易模式原理图。

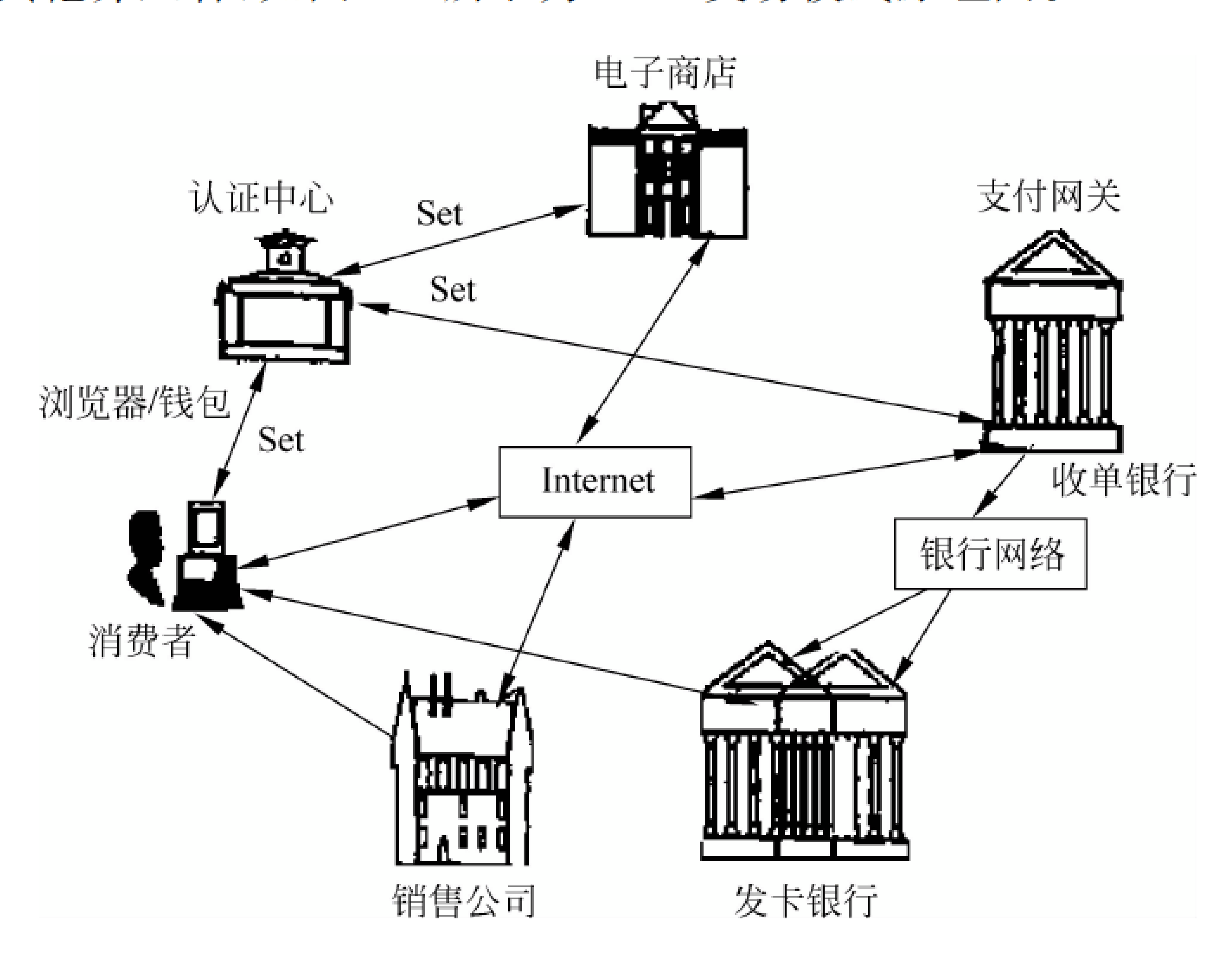


图 7-2　SET 交易模式原理图

SET 协议用于划分与界定电子商务流动中消费者、网上商家、交易双方银行、信用卡组织之间的权利义务关系,给定交易信息传送流程尺度。SET 主要由三个文件组成,分别是 SET 业务描述、SET 程序员指南和 SET 协议描述。SET 协议保证了电子商务系统中支付信息的保密性、支付过程的完整性、商户及持卡人身份的合法性,以及业务流程的可操作性。

安全套接层(Secure Sockets Layer,SSL)协议位于传输层和应用层之间,由 SSL 记实协议、SSL 握手协议和 SSL 警报协议组成。SSL 握手协议被用来在客户与服务器真正传输应用层数据之前建立安全机制。当客户与服务器第一次通信时,双方通过握手协议在版本号、密钥交换算法、数据加密算法和 Hash 算法上达成一致,然后互相验证对方身份,最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息,客户和服务器各自根据此秘密信息产生数据加密算法和 Hash 算法参数。SSL 记实协议根据 SSL 握手协议协商的参数,对应用层送来的数据进行加密、压缩、计算动态鉴别码 MAC,然后经网络传输层发送给对方。SSL 警报协议用来在客户和服务器之间传递 SSL 差错信息。

7.2　使用环境的信息安全管理

7.2.1　信息安全区

任何机构关键或敏感的信息处理设备应放置在安全的区域,由安全防御带、适当的安全屏障和准入管制手段加以保护,以防其被非法进入、毁坏或干扰。

1. 信息安全区设置

信息安全区可为上锁的办公室或物理意义的安全防御带内的房间。选择和设计安全区时,应考虑火灾、水灾、爆炸、暴乱或其他形式的自然或人为灾害所造成的损坏的可能性。同时也要考虑来自邻近场所的安全威胁等因素。根据需要对信息交接区进行隔离和管制,只允许经过授权且已辨明身份的人从楼外进入交接区。

信息安全区所有的外门和窗都要安装合乎标准的入侵检测系统，并对其进行定期检测。无人区特别要保持随时警戒；信息安全区无人时，门窗都要上锁关闭；窗户安装必要的外部保护设施。其中关键设备的放置要能够防止公众的接触；从物理上把本单位管理的信息处理设备和第三方管理的信息处理设备进行区隔；辅助设备，如复印机、传真机等，要放置在安全区内合适的位置，避免因外人接触而导致的信息泄露；危险或易燃品保存到一个离安全区适当安全距离的地方；备用设备或媒体工具应放置在离设备稍远的地方，以防主场地毁坏时同时被毁。

2. 信息安全区的实体区隔

有必要通过安全实体区隔来保护信息储存处理设施的区域，由于每个区隔都可以提供更高的安全系数，从而可以增强总体的安全水平。需要使用安全防御带来保护放置信息处理设备的区域，安全防御带即指构成区隔的东西，例如是一面墙，一道凭卡片进入的门，或值班的接待台等。每个实体区隔的位置和保护力度取决于风险评估的结果。

3. 信息安全区进出管制

在信息安全区要采取适当的出入管制，确保只有经授权的人员方可以进入。建议考虑如下的管制措施：

（1）监视或禁止来信息安全区的访问者。访问者的进入和离开资料及其时间要有记录，来访者只有在有明确经过授权的任务时才允许访问信息安全区，并要被告知信息安全区内的安全要求及紧急流程。

（2）对敏感信息和信息处理设备的通路进行管制，只有经过授权的人员才可以进入。同时使用身份识别管制手段，如刷卡或个人身份号码等对所有准入进行授权或认证。所有进入都要求有记录，并加以妥当保存。

（3）对进入信息安全区的权限要定期进行审核和更新。

4. 信息安全区内工作守则

为进一步加强已采取物理保护措施的信息安全区的安全，应制定附加的信息安全区内工作守则。这些包括针对在安全区工作的人员或第三方的管制，也包括对其活动的管制。

要求相关人员对信息安全区的存在及其内活动做到当知之则知之，不当知之则不许知之，并能够对信息安全区内所有工作进行监视；无人安全区应采取物理手段加以封闭，并定期查看；第三方人员进入信息安全区或接近敏感信息处理的设备应受限制，需要进行授权和监视。安全防御带内部具有不同安全要求的区域之间的通道要采取额外的隔离和防护措施；除非授权，否则在信息安全区内禁止使用摄影、录像、录音或其他记录仪器设备。

7.2.2 设备安全

保护设备安全的目的是防止资源的遗失、损坏、危害及正常活动的中断。设备应从物理上防止受到安全威胁或环境上的破坏。有必要对设备进行必要的保护，以降低数据被非法存取、遗失或破坏的风险。同时应考虑设备的坐落和处置，要求有特别的管制手段来保护设备免于非法使用，并对诸如电源和电缆基础设施等辅助设备进行保护。

1. 设备坐落及防护

对设备坐落加以保护，使其免受周围环境造成的威胁或损坏，并避免未经授权的进入。设备坐落要做到尽量减少不必要进入工作区的次数；敏感数据的信息处理设备和存储设备

的坐落要使其在使用时不被遗漏；需要采取管制手段来降低盗窃、火灾、爆炸、水灾、化学反应、电磁辐射等潜在威胁的风险；对可能影响信息处理设备使用的环境因素进行监控。

2. 电力供应

使设备避免断电或其他供电方面的问题。供电要符合设备制造商对供电的规定和要求，保持供电不中断的措施包括：使用多条供电线路以防某条供电线路出现故障，使用 UPS 以及备用发电机等。

支持关键运营的设备要特别考虑使用 UPS，以保证其能正常关机或持续运转。同时，要制定 UPS 发生故障时的应急计划。对 UPS 要定期检查其储电量，并按制造商的指导对其进行测试。如有必要可以使用备用发电机应对长时间断电的准备，备用发电机应当进行定期检测，要储备充足的燃料，确保发电机能随时长时间地发电。

3. 传输设备安全性

传输数据、支持信息服务的供电和通信传输设备应当受到保护，使之免于中断或损坏。如有可能，信息处理设备的线路最好铺设在地下并提供充足的备用保护措施，同时电源线和通信线要分开铺设，避免互相干扰；要防止网络电缆被非法截断或破坏，对敏感或关键设备，可考虑进一步的管制措施，如安装防护套管、冗余设备和路径、定期检查和清除线缆上的非法挂置物等。

4. 设备的维护、保养

对设备的维护应依据制造商的指示或规定的流程进行，保险条例的所有要求都要遵守，以确保设备持续正常的工作状态。根据供货商建议的周期和规格对设备进行定期维护，并且只有经过授权的人员方可对设备进行检修和维护；如设备需要送到外面维修，应采取适当的管制措施；对所有怀疑故障或实在故障及所有的防范、修正、维护措施进行记录。

5. 非管制区的设备安全管理

无论设备产权如何，使用任何单位以外的设备进行信息处理都要经单位领导批准。考虑在单位外进行信息处理可能导致的风险，在外处理信息所应采取的防护措施在程度上不得亚于单位内部的防护措施。

随时遵守制造商关于保护设备的规范，在外面以及在家工作的管制措施要经过风险评估后决定并实施；需要注意的是诸如盗窃、损坏和遗失等安全风险在各个地方的程度是不同的，因此防护措施的制定要因地制宜。

6. 设备报废或再启用安全管理

报废处置时，存有敏感信息的存储设备要从物理上加以销毁，或用安全方式对信息加以覆盖，而不能采用常用的标准删除功能来删除。

所有储存媒介在报废前都要对其进行检查，以确保其内存储的敏感信息和授权专用软件已被清除或覆盖。存有敏感数据的已损坏的存储设备要对其进行风险评估，以决定是否对其销毁、修理或遗弃。

7.2.3 日常管制

通过日常管制加以防范信息或信息处理设备被毁坏或偷窃现象的发生，防止信息和信息处理设备被非法泄露、修改或盗用，使损失或毁坏的风险降至最低。

1. 桌面及屏幕净空原则

应制定并执行桌面及屏幕净空原则，降低工作时间内和工作时间外的未经授权存取信息、遗失或损坏信息的风险。留在桌面上的信息很易于被盗，或在发生水灾、火灾、爆炸时被毁坏。可考虑实行如下原则：

在不用时，文件和计算机媒体最好锁在柜子里或其他形式的安全家具中；敏感或关键信息在不用时，特别是办公室无人时，应锁起来(最好是锁在防火保险柜或保险箱里)；个人计算机和终端及打印机在无人使用时不得置于上网状态，并要求有密码、密码锁或其他的保护措施；下班后，复印机要加以保护，禁止非法使用，敏感或机密信息打印出来后要马上从打印机上拿走。

2. 设备资源撤离

组织所属的设备、信息或软件等资源，未经授权不得私自撤离。同时，要进行场地检查以检测资源是否存在被非法挪用的情况，及时纠正违反规定的行为。

7.3 数据存取管理

根据业务和安全的要求，应当控制对信息的访问和对业务程序的访问。

7.3.1 用户访问管理

用户访问管理的目的是防止对信息系统的未经授权的访问。应当由正规的程序来控制对信息系统和服务的访问权限分配，这些程序应当覆盖用户访问全过程的所有阶段，从用户的最初注册到不再需要访问信息系统和服务的用户最终的注销。适当的情况下，应当特别注意控制特权访问权限的分配，因为这些特权允许用户超越系统控制。

1. 用户注册

为了授予对一个多用户的信息系统和服务的访问权限，应当由一个正式的用户注册和注销程序，通过正式的用户注册程序来控制对于多用户信息服务的访问。对企业内部职工，如果有未经授权的访问时要接受处罚，建议在员工合同和服务合同中包含相关规定的条款。

2. 特权管理

对系统特权的不当使用经常成为导致信息系统产生故障的一个主要因素，所以应当通过正式的授权程序来控制对特权的分配。

3. 用户密码管理

密码是一种访问信息系统或者访问时确认用户身份的常用方式。应当通过正式的管理程序来控制密码的分配，但无论如何，密码都不能以一种未受保护的形式存储在计算机上。可以使用其他的用户识别和授权技术，如指纹鉴定、签字确认和硬件标识等技术。

4. 用户访问权限的复查

为了保持对数据和信息服务的存取访问的有效控制，管理层应当实施一个正式的程序来定期复查用户的访问权限，使得用户的访问权限得到定期复查(推荐周期是6个月)并在做任何改动后进行复查；对特殊的特权访问权限应当以更高的频率来检查；推荐周期是3个月；定期核查特权分配，以确保无人得到未经授权的特权。

7.3.2 用户责任

得到授权的用户进行合作是有效的安全基础。为了维持有效的访问控制，应当让用户知道他们的责任，尤其是有关密码使用和用户设备的安全方面的责任。

1. 密码使用

用户应当按照良好的安全操作规程来选择和使用密码。密码提供了一种验证用户身份的手段，从而建立了对信息处理设备和服务的访问权限。

2. 无人值守用户设备

用户应当确保无人值守设备得到足够的保护。应当让所有的用户和合作伙伴明白无人值守设备的安全要求和安全程序，并使其清楚自己的责任。

7.3.3 网络访问控制

网络访问控制的目的是保护网络服务，控制对内部和外部网络服务的访问，这对于确保有访问权限的用户不损害这些系统的安全是必要的。为此，要确保在本组织的网络和其他组织的网络之间有适当的接口，对用户和设备有适当的授权机制，以对用户访问信息服务进行控制。

1. 网络服务的使用策略

与网络服务不安全的链接会影响到整个组织，只应当向用户提供对那些特别授权他们使用的服务进行直接访问。这种控制对于与敏感或者关键业务应用软件的联网或者与处于高风险地区的用户的联网都是十分重要的。其中高风险地区指公共的场所或者组织的安全管理范围以外的区域。当然，这一策略应当与业务访问控制策略相一致。

2. 强制路径

从用户终端到服务器的路径需要进行控制。网络被设计成要允许最大程度的资源共享和最大程度的路径选择自由，而网络的这些特征也可能为那些对业务应用软件未经授权的访问或者对信息设备未经授权的使用制造了机会。限制用户终端与允许用户访问的服务器之间路径的联合管理措施，能够降低这种风险。

强制路径的目的是防止用户选择了任何用户终端与允许用户访问的服务器之间路径的其他路径。

3. 外部连接的用户认证

外部连接可能导致对信息系统未经授权的访问。因此，应当把远程用户的访问置于比其他方式更为严密的保护之下，要从风险评估中确定所需保护的等级，这点十分重要。而且选择恰当的认证方法时也需要。

可以通过多种方式验证远程用户的身份，例如加密技术、硬件标识或者询问/应答协议。也可能用专用线路或者网络用户地址检查设备来确认连接的来源。

拨号回送程序和控制措施，能够防止对一个组织的信息处理设备的未经授权的和有害的连接，这种控制能够鉴别那些远程访问的用户。

4. 节点鉴别

自动连接到远程计算机的设备能够提供一种途径，从中可以获得对业务应用软件的未经授权的访问。因此应当认证连到远程计算机系统的连接，如果连接使用的网络在组织的

安全管理的控制范围以外，这种做法就尤其重要了。

5. 远程诊断接口的保护

应当安全地控制对诊断接口的访问。为了方便维护工程师的使用，许多计算机和通信系统安装在一个拨号远程诊断设备之中。如果未加保护，这些诊断接口就为未经授权的访问提供了途径。因此，应当用适当的安全机制对其加以保护，例如一个密码锁和一个保护程序。通过在管理员和需要访问通路的硬件/软件支持人员之间所做的安排，该程序确保了诊断接口只能由他们访问。

6. 网络隔离

网络日益被扩展到传统的组织边界以外，例如业务伙伴关系的形成可能需要互联或者共享信息处理和网络设备。网络的这种扩展可能加大使用网络的现有信息系统受未经授权的访问的风险，由于有些网络的敏感性或者关键性，它们可能需要其他网络用户的保护。在这种情形下，应当考虑在网络中引入管理措施来隔离不同的信息服务、用户和信息系统。

大型网络安全管理的方法之一就是将其分解为独立的逻辑网域，再将被连接起来以控制两个域之间的访问和信息流的两个网络之间安装一个安全网闸，形成安全边界。安全网闸可以用来过滤这些域之间的通信，并能够按照访问管理措施堵住未经授权的访问。

7. 网络连接管理

共享网络访问控制策略的要求，特别是那些跨越组织界线的关系网络，可能需要把控制措施结合起来以约束用户的连接能力。这种控制措施可以由一个用预先拟定的表格或者规则过滤通信的网络门路来实现。所用的这种约束措施应当基于访问控制策略和业务应用软件的需要，因此应当加以维护和更新。

8. 网络路径选择控制

共享的网络，尤其是那些跨越组织边界的网络，可能需要把路径选择管理措施结合起来以确保计算机连接和信息流不会破坏业务应用软件的访问控制策略。

路径选择控制应当基于确定的来源和目标地址检测机制。网络地址翻译对于隔离网络和防止路径从一个组织的网络延伸到另一个网络中也是一种非常有用的机制，它们能够在软件和硬件中实现，实施者应当清楚所配备的任何机制的作用强度。

7.3.4 操作系统访问管理

操作系统水平的安全设备应当用于限制对计算机资源的访问，这些设备应当能够鉴别和验证身份，甚至能够鉴别和验证每个经授权用户的位置和终端；记录对系统的成功访问和失败访问；提供适当的授权方式；如果使用了密码管理系统，应当能够确保使用的是优质密码；在适当的地方，限制用户的连接次数。

1. 自动终端识别

为了鉴别连到特殊地点和便携设备的连接应当考虑自动终端识别技术。如果一个会话只能从特殊的地点或者计算机终端上启动，那么自动终端识别就是一种可以考虑的方法。终端内或者贴到终端上的一个标识可以用来指示是否允许这个特定的计算机终端启动或者接收特殊事项。为保持终端标识的安全，可能需要对计算机终端进行物理保护，也可以用其他的技术鉴别计算机终端。

2. 终端登录程序

一个安全的终端登录程序应当能够获得对信息服务的访问，这一登录到计算机系统的过程的设计应当把对系统未经授权的访问的机会降到最低限度。因此为了避免给未经授权的用户以不必要的帮助，该登录程序只会透露出最少的系统信息。一个好的登录程序应当做到符合相关规范，如在登录程序中不提供可能会帮助未经授权的用户的信息；能够限制所允许失败登录的次数，并记录失败的尝试；在重新登录之前强制等待一段时间或者拒绝任何没有特殊授权的进一步尝试，限制所允许的登录程序的最长和最短时间，如果超过了这个范围，系统应当终止登录等。

3. 用户识别和鉴定

所有的用户应当有唯一的标识(用户 ID)供他们个人并且只供他们个人使用，这样就可以追踪各种活动到负有责任的个人身上。在例外的情况之下，可能会让一个用户群或者特殊的工种共享一个用户 ID，管理层对这种情况的批准应当记录在案。

需要有各种授权程序来证实用户所声称的真实身份。密码是一种非常通用的进行识别和鉴定的方法，这一方法基于一个只有用户才知道的秘密。利用加密技术和鉴别协议也可以达到同样的目的。存储标识或者用户拥有的智能卡这类物品也可以用来进行识别和鉴定。利用个人的唯一特征或者属性的生物鉴别技术也可以用来鉴别一个人的身份。将鉴别技术和管理机制妥善地结合到一起能够得到更为强大的鉴定能力。

4. 密码口令管理系统

密码是验证用户访问计算机权限的主要形式之一，密码管理系统应当提供一个有效的、交互的设备，这样可以确保优质密码。一些应用程序需要有独立的职权来分配用户密码，在大多数情况下，密码是由用户选择和维护的，一个好的密码管理系统应当符合密码管理的标准和规范。如输入密码时不要将其在屏幕上显示出来，把密码与应用软件系统的数据分开存放，以使用单向加密算法的加密形式存储密码口令等。

5. 系统实用程序的使用

大多数计算机安装有一个或者更多系统实用程序，它们可能有能力超越系统和应用程序的控制，因此限制并严格控制对它们的使用是十分重要的。

系统实用程序的使用有必要配置认证程序，并把系统实用程序从应用软件中分离出来；把使用系统实用程序的人限制在最少的值得信任的授权用户之内，要为系统实用程序的特殊使用进行授权；需要限制系统实用程序的有效性，并要记录系统实用程序的所有使用；所有基于软件的多余实用程序和系统软件需要删除。

6. 终端暂停

为了防止未经授权人的访问，在一段确定的休止期结束后，应当关闭在高风险地区的暂停终端或者是正在为高风险系统提供服务的终端。在一段确定的暂停期后，这一终端暂停手段应当清除终端屏幕内容并关闭应用程序和网络会话。

7. 连接时间的限制

对连接时间的限制应当为高风险应用程序提供额外的安全保证，限制终端的连接时间可以减少未经授权访问的空间。对于敏感的计算机应用程序，特别是那些安装在高风险地区的终端，应当考虑这样的管理措施。这样约束措施的例子包括使用预先确定的时间段，例如批量的文件发送，或者定期的短时交互式对话；如果没有超时或者延时业务，限制连接到

正常办公时间的次数等。

7.3.5 应用程序访问控制

防止保存在信息系统内的信息被未经授权访问，应当使用安全设施限制在应用程序系统中的访问，对软件和信息的逻辑访问应当限制在经过授权的用户之中。

1. 应用软件系统限制

能够控制用户对信息和应用程序系统功能的访问，并要与确定的业务访问控制策略相一致；为任何一个能够超越系统或应用程序限制的实用程序和操作系统软件提供保护，防止未经授权的访问；不损害有共享信息资源的其他系统的安全；只能够向所有权人、其他被指派和经授权的个人或者确定的用户群提供对信息的访问权限。

2. 信息访问限制

按照确定的访问控制策略，应当为应用软件系统的用户包括技术支持人员提供对信息和应用程序系统的访问。

通过适当编辑用户文件，可以限制用户对未得到授权访问的信息或者应用程序系统功能的了解；控制用户的访问权限，例如读取、改写、删除和执行等权限；确保处理敏感信息的应用程序系统的输出只包括与使用相关的信息，而且只送到得到授权的终端和地点，包括对这种输出周期性的复查，以确保多余的信息被删除。

3. 敏感系统的隔离

敏感系统可能需要专用(隔离)的计算环境。有些应用程序系统对于潜在的损失如此敏感以至于需要对它们做专门处理，这种敏感性可能表示应用程序系统应当在专用计算机上运行，而且只同受信的应用程序系统共享资源，或者没有限制。

对一个应用程序系统的敏感性应当做清楚的定义，并且应用程序的所有权人应该被记录在案。当一个敏感的应用程序在共享的环境下运行时，应该能够被识别，并获得敏感应用程序的所有权人的准许。

7.3.6 检测系统访问和使用

系统中偏离访问控制策略的行为应能被监控和记录，以便在发生安全事件时提供证据。系统检测允许对所采用管理措施的有效性进行检测，并允许对一个访问策略模型的确认进行验证。

1. 事件记录

应当编写用来记录异常现象和其他有关安全事件的审查日志，并在各方同意的时间段内保持该日志，以协助以后的调查研究和访问控制监测。审核日志需要放入档案中，或作为记录保留策略的一部分，或出于搜集证据的需要。

2. 检测系统使用

(1) 程序和风险区域

为了确保用户只做得到明确授权的行为，信息处理设备使用的检测程序是必需的，并应经风险评估以确定个人设备所需的监测等级，确定用户得到授权的访问细节，如：用户 ID、关键事件发生的日期和时间、事件的类型、访问的文件、使用的程序/实用程序、所有有特权的作业、未经授权的访问尝试、系统警报或者故障等。

（2）风险因素

应当定期检查监测活动的结果，检查的频率取决于所涉及的风险。应当加以考虑的风险因素包括：应用进程的重要程度，所涉及信息的价值、敏感性和重要程度，以往的系统过滤和误用的经验教训，系统互联的程度等。

（3）记录和检查事件

日志检查涉及对于系统所面临威胁的理解和对这些威胁可能的产生方式的认识。系统日志常常包含大量的信息，其中很多信息与安全检测无关。出于安全检测的目的而帮助识别重要事件时，应当考虑把适当的信息类型自动复制到第二个日志，或者使用适当的系统实用程序或检测工具，以便进行文件审查。

当为检查日志而分配责任时，应当考虑把执行检查的人员和其活动被监测的人员的角色分离开。尤其应当注意日志记录设施的安全性，因为一旦遭到破坏可能给人一种十分安全的假象。

7.3.7 移动计算和远程工作

使用移动计算时，应当考虑在未经保护的环境下工作的风险，并且要采用适当的措施。在远程工作时，应当为远程工作地点提供保护，并且确保对这种工作方式有适当的安排。

1. 移动计算

使用移动计算设备时，应当特别注意确保业务信息不受损害。应当采取正式策略来考虑使用移动计算设备的风险，特别是在未加保护的环境之中。例如，该策略应当涵盖物理保护、访问控制、加密技术、备份文件和防范病毒等方面的需要。该策略还应当包括有关把设备连接到网络的规则和建议，以及对于在公共场所使用这些设备的指导。

在保护范围之外的未受保护的区域，在适当的位置应当有保护措施，以避免未经授权的访问或者泄露由这些设备存储和处理的信息。对连接到网络的移动设备给以适当的保护，只有经过成功的识别和鉴定之后，才可以使用移动计算设备通过公众网对业务信息进行访问，并且有适当的访问控制机制在。还应当对移动计算设备加以物理上的保护，以防在离开时被偷窃。应当训练职工使用移动设备，提高他们对这种工作方式所带来的额外风险和应当实行的管理措施的认识。

2. 远程工作

远程通信技术能够让员工在组织之外的远程地点工作，但应该对远程工作进行保护，以防止设备和信息被盗走、信息未经授权就披露、对内部系统的未经授权的访问或者设备的误用。远程工作不但需要授权，还要由管理层控制，而且对这种工作方式应当有适当的安排。应当考虑开发一种策略、程序和标准来控制远程工作活动。

7.4 容灾管理

7.4.1 容灾的概念

容灾是指为了保证关键业务和应用在经历各种灾难后，仍然能够最大限度地提供正常服务所进行的一系列系统计划及建设行为。业务连续性是容灾的最终建设目标。容灾是一

个宏观的概念，通常所说的容灾系统、灾难恢复等只是容灾的一部分，或者说是容灾发展历程中的某一阶段的雏形。事实证明，只有对数据存储备份制定完备、持续且可执行的容灾计划，特别是业务连续计划，才能为人们提供万无一失的数据安全保护。

严格地说，容灾计划包括一系列应急计划，如业务持续计划(Business Continuity Plan，BCP)、业务恢复计划(Business Recovery Plan，BRP)、运行连续性计划(Continuity of Operations Plan，COOP)、事件响应计划(Incident Response Plan，IRP)、场所紧急计划(Occupant Emergency Plan，OEP)、危机通信计划(Crisis Communication Plan，CCP)、灾难恢复计划(Disaster Recovery Plan，DRP)等。

在技术层面上，容灾需要考虑以下内容。

- 数据版本保护：建立容灾的多版本保护底线。
- 实时数据保护：数据复制，近乎0的数据丢失，数据一致性。
- 应用系统恢复：恢复时间(包括数据库恢复)、应用版本的一致性等。
- 网络系统恢复：数据访问点变化、建立新网络路径、动态路由(收敛时间/稳定性)。
- 容灾切换决策：及时发现灾难(容灾系统管理)、容灾切换的损失和补救办法。
- 容灾切换过程：变更管理。

容灾不只是简单备份，也不仅仅是技术，完善的容灾管理方案对解决容灾问题具有非常重要的意义。这种管理包括三个方面，即对容灾环境的管理、存储资源的管理和数据备份的管理。

7.4.2 容灾环境管理

小型的容灾系统一般采用手工备份或简易的DAS、NAS方式进行数据存储备份，而在大型的容灾系统中，更高的数据传输速率、不依赖服务器、数据吞吐量更大的SAN得到了更多的应用。一个复杂的存储系统往往是由DAS、NAS和SAN等多种存储方式共同组成，要有效地解决容灾问题，就需要将这些复杂、异构的存储设备进行统一、集中的管理，也就是对容灾环境进行管理。

由于SAN在目前尚未有统一的标准，不同硬件厂商的产品存在一定的兼容性困难，因此，在规划一个大型容灾系统的存储环境时，对SAN的管理显得尤其重要。CA公司的BrightStor SAN Manager软件则是一个可以有效管理复杂、异构条件下的容灾环境的产品。

7.4.3 存储资源管理

存储资源管理主要解决两个方面的问题，一是确保容灾恢复时的数据可用性，二是随时掌握容灾系统的情况，保证容灾系统的可靠性和控制成本。可以想象，如果容灾系统出现故障却不为人所知，或者发现了故障却不能及时解决，即使是性能最好的容灾系统又有什么用呢？

1. SRM存储资源管理系统

CA的BrightStor Storage Resource Manager(SRM)可以对容灾系统的存储资源和数据恢复进行有效的管理。BrightStor是一整套企业级的智能化存储管理解决方案，定位在存储硬件设备和上层应用之间，通过各种集成化的产品和工具为驻留在企业任何位置的数

据提供全方位的、有效的存储管理和保护。

1）基础存储应用管理

BrightStor 通过提供数据可用性和企业存储资源管理两个方面的解决方案来实现对用户基础存储应用的全面管理。

（1）数据可用性管理

CA 的数据可用性管理解决方案始终确保服务器、应用和数据的可用性。CA 是目前唯一能够为用户提供从笔记本到大型主机、从 LAN 到 SAN 中的各种数据保护的存储软件供应商。这些解决方案可以为全球任何规模的企业实现跨平台的综合数据备份/恢复以及层次存储管理。另外，CA 的数据可用性管理解决方案还涵盖了使用 z/OS、OS/390、z/VM 和 VSE 等大型主机系统的企业服务器环境的数据可用性管理。CA 的数据可用性管理解决方案主要包括 BrightStor Enterprise Backup、BrightStor Mobile Backup 和 BrightStor ARCserve Backup。

（2）企业存储资源管理

CA 的企业存储资源管理解决方案通过提供事件管理、报表、趋势图、预测和分析等各种使用方便的管理手段来充分利用存储资源。企业可以通过利用诸如 SAN 管理、存储资源管理、磁带管理、软件虚拟磁带等各种 BrightStor 存储管理解决方案来有效地管理和控制存储硬件和人工的成本，从而降低总体拥有成本。

2）存储管理门户的单点管理

在这些数据应用解决方案的基础上，BrightStor 提供了集中式的存储管理门户，帮助企业在已有的存储架构中，整合不同生产主机平台的数据资源，通过统一的界面管理各种应用软件和数据库，真正实现集中化的、智能的、便捷的单点存储管理。这个门户产品就是 BrightStor Portal。

BrightStor Portal 从根本上简化了跨多种协议和多供应商硬件环境的存储管理，确保了存储资源的最有效利用。通过 BrightStor Portal，BrightStor 的各种单点控制功能，包括查找和发现数据、监测存储设备、进行备份和恢复等操作、决策、预测，都可统一完成。此外，BrightStor Portal 还可简化各种存储操作。通过直观、简洁的 Web 网页风格的界面，管理员只需轻松点击鼠标，就可方便地实现存储应用中的各种操作，而无须了解数据具体存储在哪里，或者如何存储。

BrightStor Portal 是一个灵活、可扩展的平台，是 CA“无边界的存储管理”理念的重要体现。通过开放的、标准友好的解决方案，BrightStor Portal 增强了 CA 在异构环境集成方面一贯的领导地位。它可以通过轻松定制，为新的供应商、设备、应用和各种协议提供支持，也可以进一步扩展，以适应甚至是最大型的、拥有最多种不同企业存储资源的环境。

2. BrightStor 适用的网络存储架构

无论何种类型的企业，无论企业采用的是哪一种网络存储架构，CA 的 BrightStor 系列端到端存储管理解决方案都能通过各种集成化的产品和工具来提供支持。BrightStor 支持当前流行的网络存储架构，包括直接附加存储(Directed Attached Storage，DAS)、存储区域网络(Storage Attached Network，SAN)和网络连接存储(Network Attached Storage，NAS)。

1）DAS

DAS 方式一直是大多数服务器采取的方式。从严格意义上讲，DAS 不属于网络存储

系统。服务器通过专用路径(典型的如 SCSI)将存储设备连接起来,需要访问时,它发出 I/O 指令给存储设备,存储设备根据指令进行相应操作,将数据返回给服务器,或者将服务器的数据写入到磁盘。DAS 的存储设备可以是磁盘驱动器,也可以是 RAID 子系统,或者其他存储设施。通常 DAS 与服务器之间提供块级接口,数据的传输以块为单位。这种方式结构简单,成本比较低,但扩展性差,数据共享困难,只适合短距离传输。

2) SAN

SAN 是一种高速、专用网络,用于连接服务器和存储设备,基于这种网络技术的存储结构,具有很高的性能。在这种结构中,多台服务器连接到一个内部高速网络 SAN 上,多个存储设备也连接到这个网络上。SAN 网络通常使用 Fiber Channel(光纤通道)作为介质,使用交换技术在服务器和存储设备间建立传输通道,可以提供高达 2.5Gbps 的数据传输速率,因此 SAN 网络连接存储能提供非常高的带宽。这对于大容量的数据存储是必不可少的。基于 SAN 结构的存储系统的性能和成本较高,具有良好的扩展性,但管理复杂。

3) NAS

与以上两种方式不同,NAS 通过通用的网络,将本地服务器与远程的 NAS 存储设备连接起来。远程的 NAS 存储设备是一个智能设备,它带有自己的文件系统,将本地文件系统以工业标准的网络文件系统(最常用的包括 NFS 和 CIFS)的方式提供给服务器,即对 NAS 设备的访问以文件为单位。服务器通过将远程的文件系统安装到本地的文件系统层次上,透明地访问远程文件。NAS 提供一种开放的数据访问方式,可以更好地支持多种操作系统平台和硬件平台。NAS 具有低廉的成本,其网络延迟较大、带宽较低,属于文件级的访问,具有开放的标准接口,管理简单。

7.4.4 数据备份管理

数据备份是容灾的基础,是指为防止系统出现操作失误或系统故障导致数据丢失,而将全部或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质的过程。容灾系统包括备份中心、备份设备和备份数据等部分,专业的数据备份系统是容灾不可或缺的重要组成部分,而只有 Windows 和应用系统本身自带的备份工具是远远不够的,没有优秀的备份解决方案,根本谈不上容灾的实现。

1. 常见的备份方式

(1) 定期磁带备份数据

- 远程磁带库、光盘库备份。即将数据传送到远程备份中心制作完整的备份磁带或光盘。
- 远程关键数据+磁带备份。采用磁带备份数据,生产机实时向备份机发送关键数据。

(2) 远程数据库备份

这种方式是在与主数据库所在生产机相分离的备份机上建立主数据库的一个拷贝。

(3) 网络数据镜像

这种方式是对生产系统的数据库数据和所需跟踪的重要目标文件的更新进行监控与跟踪,并将更新日志实时通过网络传送到备份系统,备份系统则根据日志对磁盘进行更新。

(4) 远程镜像磁盘

通过高速光纤通道线路和磁盘控制技术将镜像磁盘延伸到远离生产机的地方,镜像磁盘数据与主磁盘数据完全一致,更新方式为同步或异步。

数据备份必须要考虑到数据恢复的问题,包括采用双机热备、磁盘镜像或容错、备份磁带异地存放、关键部件冗余等多种灾难预防措施。这些措施能够在系统发生故障后进行系统恢复。但是这些措施一般只能处理计算机单点故障,对区域性、毁灭性灾难则束手无策,也不具备灾难恢复能力。

2. 目前常用的数据备份方案

目前常用的数据备份方案有 LAN 备份、LAN Free 备份和 SAN Server-Free 备份三种。LAN 备份针对所有存储类型都可以使用,LAN Free 备份和 SAN Server-Free 备份只能针对 SAN 架构的存储。目前主流的备份软件,如 IBM Tivoli 、Veritas 均支持上述三种备份方案。下面介绍的是 SRM 支持的备份方案。

(1) DAS 备份方案

BrightStor 为 DAS 架构提供了多种存储设备(磁带、磁盘等)的管理与使用、自定义备份策略、自动执行备份作业、数据压缩和解压、数据加密和解密等功能,可满足企业管理 DAS 架构的需求。

如图 7-3 所示为典型的 DAS 备份方案。该方案用一台与磁带机相连的服务器作为备份服务器,并安装 BrightStor Enterprise Backup Server 软件,以及 BrightStor Tape Library 选件,可实现 UNIX、Windows NT、AS/400 的跨平台备份。

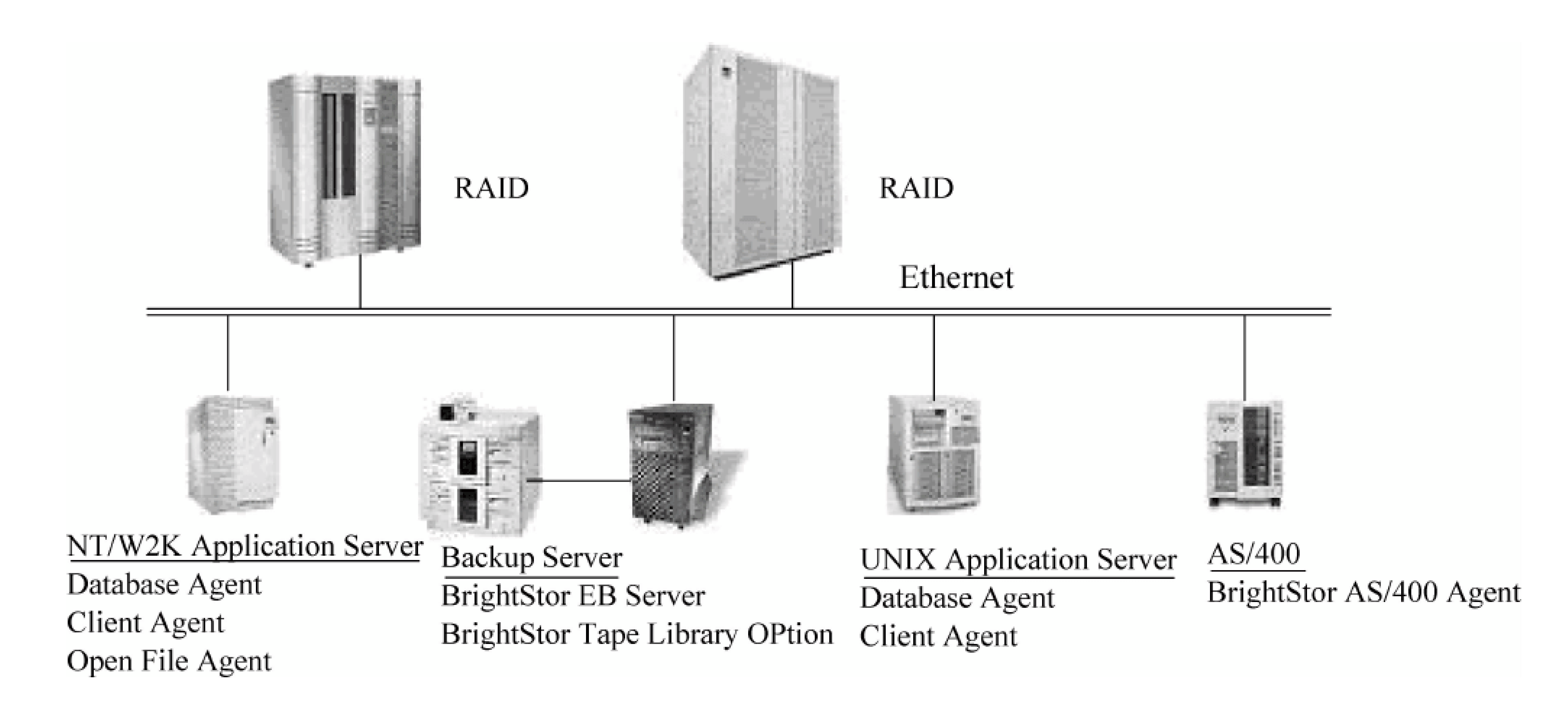


图 7-3 DAS 备份方案

利用该解决方案,以往要通过复杂操作才实现的任务现在都可通过 BrightStor 提供的简单的操作界面实现。因为 BrightStor 可以自行运行和管理,极少需要用户的干预,能够自动安排和执行数据的全备份和增量备份,因此可帮助客户降低维护成本,同时避免人为操作上的错误发生,增加备份的可靠性。此外,在对硬件的操控方面,BrightStor 不仅对客户的多个介质单元具备极高的容错能力,还实现了自动对磁带机使用情况进行跟踪和清理等功能。这些都很大程度地提高了 IT 管理的效率并降低了成本投入。

(2) NAS 备份方案

NAS 是网络中心型存储技术,提供用户基于网络快速访问数据的能力。NAS 的出现标志着存储技术迈上了一个新的台阶,从此,网络存储日益流行起来。如图 7-4 所示为一个典型的 NAS 备份方案。BrightStor Enterprise Backup 安装在生产主机上,当生产主机上的数据需要备份时,BrightStor Enterprise Backup 可以发出 NDMP(Network Data Management Protocol)指令,将备份提交到 NAS 服务器,然后由 NAS 服务器控制磁盘阵列、磁带机进行数据备份。这样进行数据备份的好处是 NAS 服务器可以将数据直接从本地硬盘移到磁带库,从而避免占用生产主机的资源,这也就是所谓的无服务器备份。

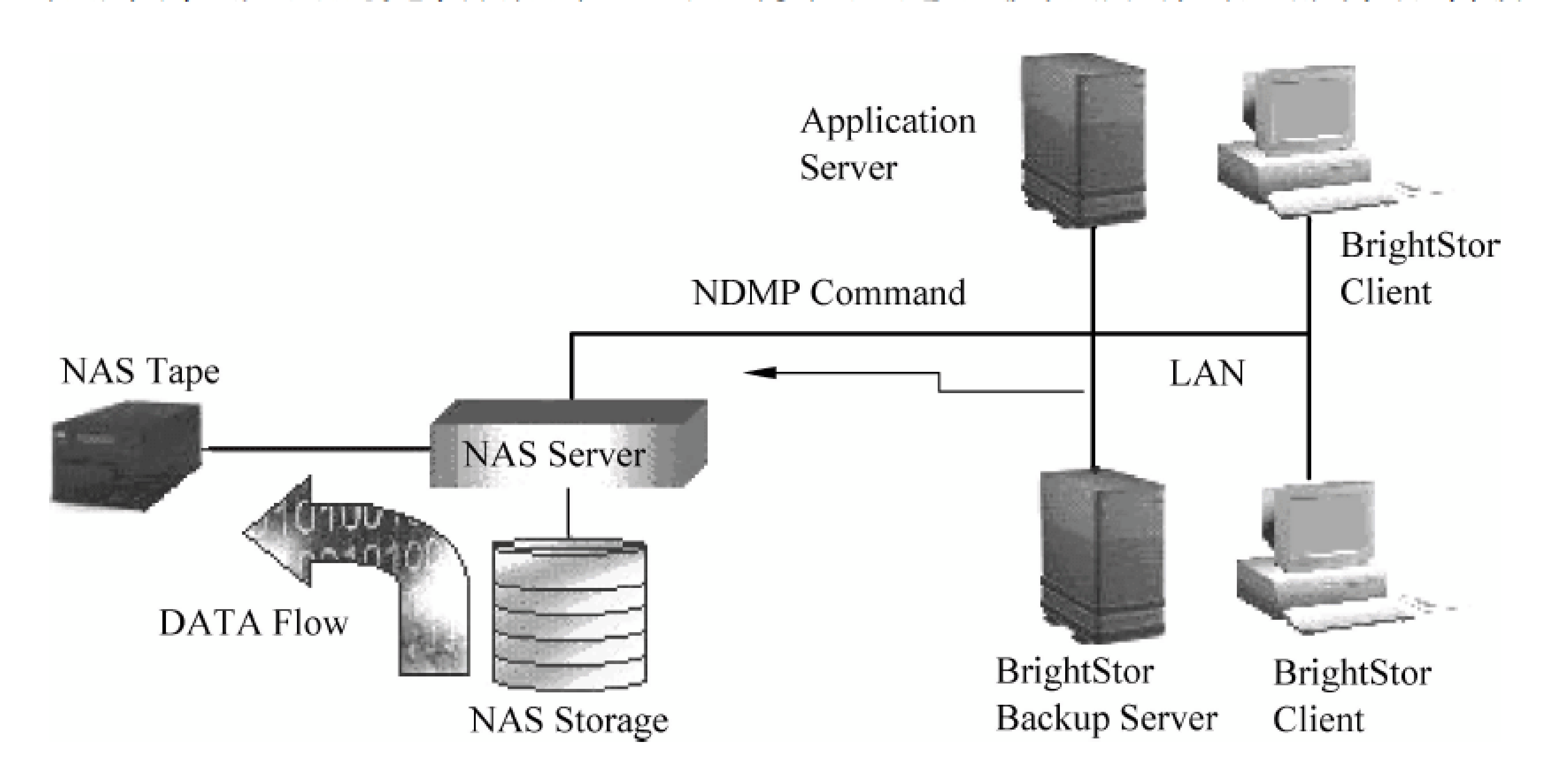


图 7-4 NAS 备份方案

CA 的 NAS 备份方案可显著提高备份的速度,确保客户的关键数据资产一天 24 小时×一周 7 天可用。同时它还具有领先的集中管理和报告功能,使管理员可以更加主动地去管理数据备份和存储过程,提高管理的效率。此外,该方案还具有很好的可扩展性,可满足企业不断扩展的业务需求。

(3) SAN 备份方案

与 LAN、NAS 相比,SAN 可以更好地满足企业对存储设备的性能、可用性、可扩展性,以及灵活性的要求。CA 的 SAN 方案可以为企业更好地管理 SAN 架构提供许多先进的管理功能,包括自动的 SAN 架构发现、SAN 设备的访问和控制、先进的 SAN 可视化管理,以及其他存储管理功能的集成等。如图 7-5 所示为一个典型的 SAN 备份方案,在该方案中,BrightStor Enterprise Backup、BrightStor ARCserve Backup、BrightStor Mobile Backup 等备份软件安装在生产主机和工作站上。生产主机上的数据会通过光纤协议集中到一个 SAN 交换机上,然后由该交换机把数据转移到路由器上,再由路由器来控制磁带库进行数据备份,或直接由交换机控制磁带库进行备份。

从这个方案可以看出,CA 的 SAN 备份方案可以将众多的服务器和工作站进行集中管理,从而降低存储管理的成本,并且可以将备份数据流从 LAN 迁移到 SAN,从而缩短备份/恢复时间并减少 LAN 的拥挤,提高备份的效率。该方案还具有几乎无限的可扩展性,使客户可以根据业务发展需求方便地进行扩展,最大限度地利用他们在存储设备上的投资。

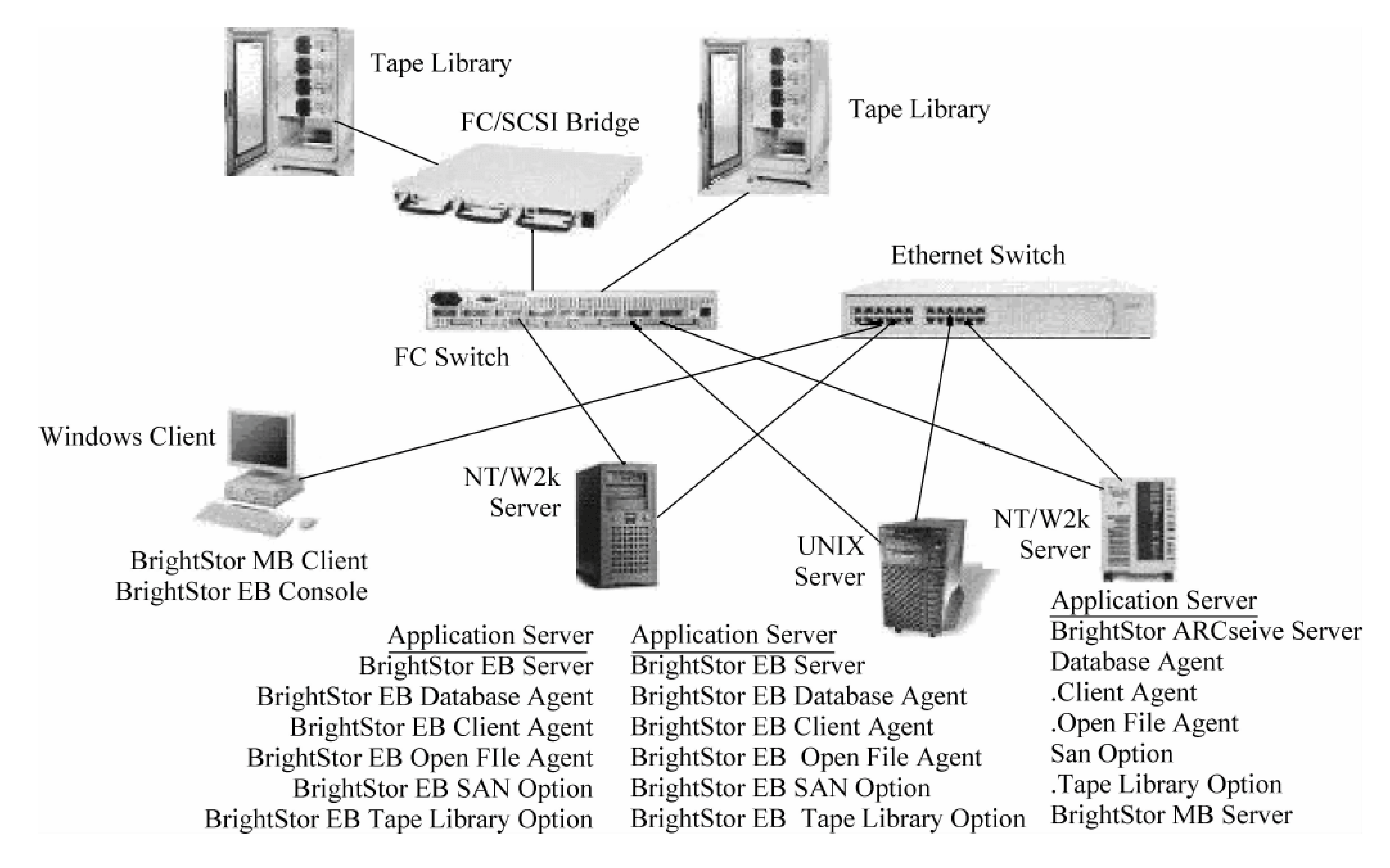


图 7-5　SAN 备份方案

7.5　本 章 小 结

本章介绍了信息安全管理的相关知识，首先介绍了信息安全管理的概念，包括信息安全、信息安全的威胁、信息安全管理等内容；然后介绍了使用环境的安全管理，对安全环境诸要素进行了讨论；数据存取和容灾管理是信息安全管理中的重要内容，最后对数据存取控制和容灾管理方案进行了介绍。

通过本章的学习，需要了解信息安全的威胁因素和安全措施；理解安全管理的重要性、策略和方法；掌握数据存取和容灾的应用技术。

习　题　7

一、选择题

1. 一般认为，目前网络信息安全面临的威胁主要表现在(　　)三大类。

A. 信息泄露　　B. 信息欺骗　　C. 拒绝服务　　D. 信息破坏

2. 信息安全的特征不包括(　　)。

A. 保密性　　B. 完整性　　C. 可用性　　D. 标准性

3. 计算机网络安全措施包括保护网络安全、保护应用安全和(　　)三方面。

A. 保护系统安全　　B. 保护设备安全

C. 保护目录安全　　D. 保护文件安全

4. 数字签名机制提供了一种鉴别方法，以解决(　　)等问题。

A. 伪造　　B. 抵赖　　C. 冒充　　D. 篡改

5. 数字证书的最主要构成包括一个用户公钥、密钥所有者的(　　),以及被信任的第三方签名。

A. 私钥　　　　B. 算法

C. 身份标识符　　　　D. 身份等级信息

6. 如果把文件夹的安全属性设为“只读”,这种访问控制方式为(　　)。

A. 目录　　B. 属性　　C. 入网　　D. 操作权限

二、简答题

1. 什么是信息安全和信息安全管理?

2. 信息安全的威胁有哪些?

3. 如何理解信息安全的重要性?

4. 访问控制策略有哪些?

5. 什么是容灾管理?

6. 使用环境的安全管理包括哪些内容?

7. 什么是 DAS、NAS 和 SAN?

8. 在 Windows Server 2003 中实现备份功能,包括活动目录、服务状态信息、磁盘配额、注册表、IIS、DHCP、DNS、WINS 等内容的备份。

第8章 网 络 管 理

目前，网络系统的维护与管理工作变得日趋繁杂，仅靠人工管理的方法是无法可靠、迅速地保障网络的正常运行的。因此迫切需要用计算机，也就是网络管理系统来进行网络管理。

8.1 网络管理系统

8.1.1 网络管理系统概述

1. 网络管理系统的概念

网络管理系统就是实现网络管理的各种功能的软、硬件系统，它可以是一个计算机系统，也可以是一个网络化系统。网络管理的对象一般包括路由器、交换机、hub 等。近年来，网络管理对象有扩大化的趋势，即把网络中几乎所有的实体，如网络设备、应用程序、服务器系统、辅助设备（如 UPS 电源）等都作为被管理对象。网络管理系统可以给管理员提供一个全面系统的网络视图。

2. 网络管理系统的分类

网络管理系统软件并没有完全统一的分类标准，总体来说，网络管理软件可以有以下几种分类标准。

（1）按照发展历史分类

根据网络管理系统的发展历史，可以划分为三代。

第一代网络管理系统就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。如路由器和智能交换机中的配置和管理命令。

第二代网络管理系统有着良好的图形化界面，用户无须过多了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控，大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题，容易引发误操作。

第三代网络管理系统相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。而且通常是采用 B/S 架构，一方面可实现远程管理，另一方面实现起来非常容易，只要有浏览器即可。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网络管理系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源。

（2）按照管理对象分类

目前常用的网络管理软件可分为两大类，主要根据管理对象划分，即通用网络管理软件

和网元(网络设备)管理软件两大类。网元管理软件只管理单独的网元(如交换机、路由器、服务器等),通用网络管理软件的管理目标则是整个网络。

网元管理软件一般由设备厂商提供,各厂商采用专有的管理 MIB 库,以实现对厂商设备本身的细致入微的管理,包括可以显示出厂商设备图形化的面板等,如安奈特公司的 AT-View Plus、思科公司的 Cisco View 和华为网络公司的 Quidview 等。

通用网络管理软件则主要用于掌握全网的状况,作为底层的网管平台来服务于上层的网元管理软件等。如安奈特公司的 AT-SNMPc,可以提供一个第三方的网管平台,支持对所有 SNMP 设备的发现和监控,可集成厂商设备的私有 MIB 库,实现对全网设备的统一识别和管理。从而避免了厂商专用型网络管理系统无法实现对全网设备的统一管理,用户往往采用多台网管工作站分别安装不同的系统,进行分别管理的局限性,有利于简化管理和降低成本。这类产品还有惠普公司的 HP OpenView、CA 公司的 Unicenter、IBM 公司的 Tivoli NetView 等。国内的如游龙科技的 SiteView、网强信息技术公司的网强网管等。

(3) 按照管理范畴分类

从网络管理的范畴来分类,又可分为对网"路"的管理(即针对交换机、路由器等主干网络进行管理)、对接入设备的管理(即对内部 PC、服务器、交换机等进行管理)、对行为的管理(即针对用户的使用进行管理)、对资产的管理(即统计网络系统软、硬件信息)进行管理等。

(4) 按照管理功能分类

根据国际标准化组织的定义,网络管理有 5 大功能:故障管理、配置管理、性能管理、安全管理、计费管理。根据网络管理软件产品功能的不同,又可细分为 5 类:网络故障管理软件,网络配置管理软件,网络性能管理软件,网络服务/安全管理软件,网络计费管理软件。不过,其实现在大多数网络管理软件都是以上部分或全部功能的集合,单一功能的比较少见。

8.1.2 网络管理系统的结构与组成

1. 网络管理系统的逻辑组成

从逻辑上,网络管理系统可以分为管理对象、管理进程、管理信息库和管理协议 4 个部分;从逻辑位置来说,可以划分为网内的网络管理系统和网外的网络管理系统,即网络管理系统置于被管网络之内或之外。

(1) 管理对象是经过抽象的网络元素,对应于网络中具体可以操作的数据,如记录设备或设施工作状态的状态变量、设备内部的工作参数、设备内部用来表示性能的统计参数等。

(2) 进程管理是负责对网络中的设备和设施进行全面的管理和控制的软件,根据网络中各个管理对象的变化来决定对不同的管理对象采取不同的操作。

(3) 管理信息库用于记录网络中管理对象的信息,如状态类对象的状态代码、参数类对象的数值等。它要与网络设备中的实际状态和参数保持一致,能够真实地、全面地反映网络设备或设施的情况。

(4) 管理协议负责在管理系统与管理对象之间传递操作命令,并负责解释管理操作命令。实际上,管理协议也就是保证管理信息库中的数据与具体设备中的实际状态、工作参数保持一致。

网络管理系统的功能按作用分为以下三个部分:

- 操作：包括系统配置、运行状态显示、操作控制、告警、统计、数据的收集和存储、安全控制等。
- 管理：包括网络配置、软件管理、计费和账单生成、服务分配、数据收集、网络数据报告、可用性分析、性能分析、支持工具和人员、资产、规划管理等。
- 维护：包括网络测试、故障告警、统计报告、故障定位、服务恢复等。

网络管理系统的组织如图 8-1 所示。

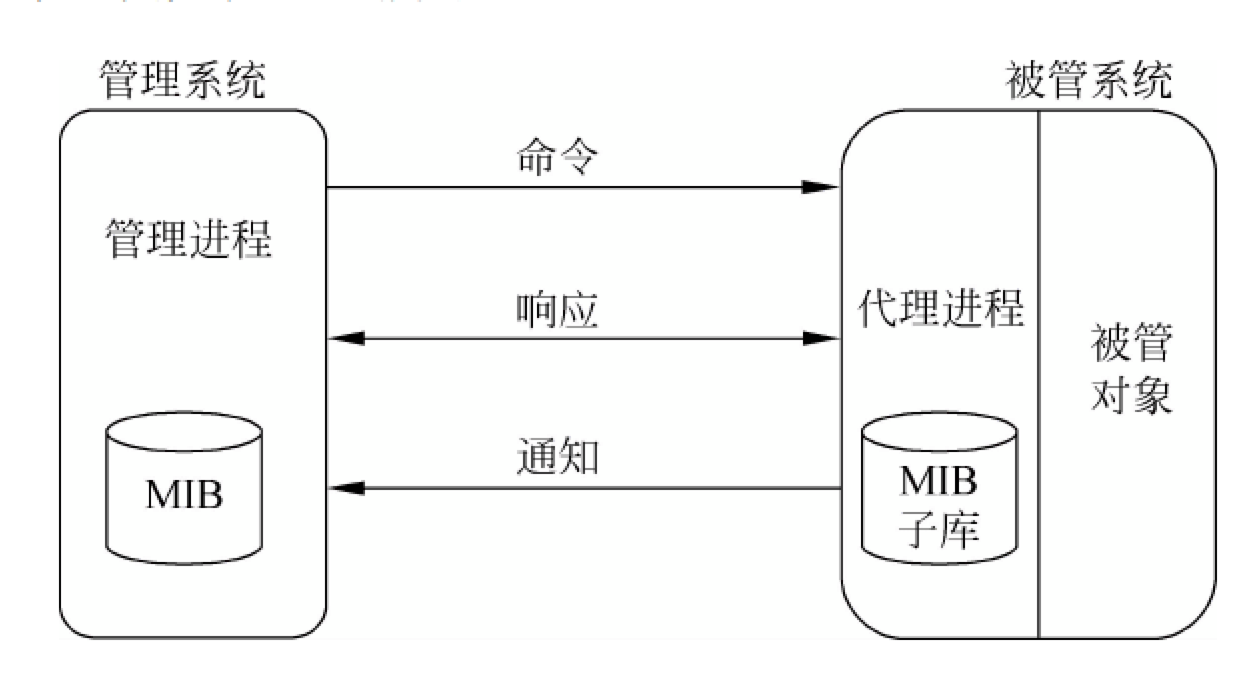


图 8-1　网络管理系统的逻辑组成

2. 网络管理系统的结构

一个网络管理系统通常包括网络中各种参数的测试与采集、信息组织与管理、功能设置、网络管理的决策与操作应用等，它们间的关系如图 8-2 所示。

管理决策与操作

网络管理系统功能的设置

管理信息的组织与管理

网络系统参数测试与采集

网络系统

图 8-2　网络管理系统组成部分的结构关系

(1) 网络系统参数的测试与采集

每一个层次都对上一个层次提供支持服务，但是网络信息的生成是网络管理系统的基础。网络参数是网络各种条件和各种状态的反映，从这些参数可以获得网络的状态特性，因此网络参数的获得是网络管理的重要步骤。

获得网络参数的方式是多种多样的，一般情况下诸如配置、数量、运行条件等静态信息是比较容易获得的，要获得网络运行的动态信息需要对网络进行测试，并进行相应的计算和处理后方可得到。

(2) 管理信息的组织与管理

MIB 是用于网络管理功能实现的信息集合。在 MIB 中，被管理网络和其管理信息通常用被管对象来表示。被管对象包含着关于网络及被管对象相应管理行为和作用的信息。MIB 提供了执行查询、实现被管对象操作、处理事件管理及建立被管对象间关系的信息基础。管理员通过查询 MIB 中的内容就可获得有关设备和系统的各种状态信息。

MIB 一般包括三个部分，即访问服务、构造服务和支持服务。构造服务建立在支持服务之上，访问服务又是建立在构造服务之上的。

访问服务主要提供访问 MIB 中被管对象信息的编程接口；构造服务提供将管理应用中被管资源表示成被管对象的定义手段；支持服务提供 MIB 的永久存储及资源的管理。

(3) 网络管理系统功能的设置

网络管理系统是由多个子系统组成的，而这些子系统是具有各种不同功能的集合，建立网络管理系统之前，必须确立各个网络管理子系统功能的集合。而网络管理系统功能的确定通常通过网络管理需求分析、子网生存状态和网元结构状态、被管对象的管理信息基础和条件、各子系统间的关系等方面来确定。

3. 网络管理系统的组成

从网络管理功能的应用角度来看，网络管理系统由管理应用和底层服务软件系统组成，如图 8-3 所示。

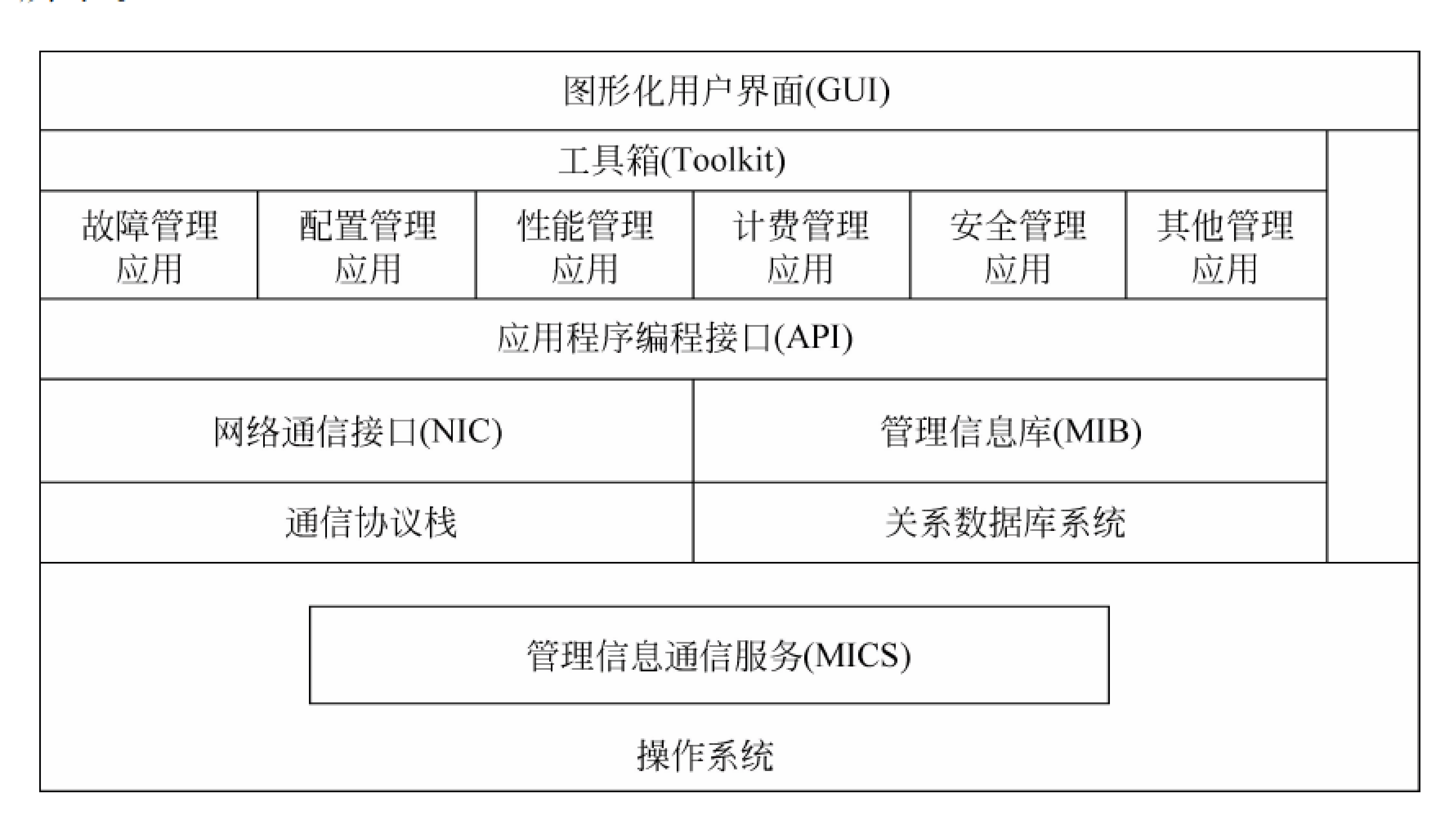


图 8-3　网络管理系统组成实例

(1) 图形化用户界面(GUI)

用户界面(User Interface，UI)是指网络管理员与设备间的接口，它涉及所有的输入输出方式。图形化用户界面(Graphical User Interface，GUI)是指采用图形方式显示的计算机操作用户接口。与早期计算机使用的命令行界面相比，图形界面对于用户来说在视觉上更易于接受。

GUI 可以提供文本/图形方式的信息交流，使管理员尽可能自然地控制管理应用，有利于以直观的方式从网络管理系统有效地得到管理信息。它是网络管理系统中直接面向网管用户的软件系统，网络管理应用与图形化用户界面的结合，构成了相应的网络图形化管理工具。

(2) 网络通信接口(NCI)

网络通信接口提供被管网络与管理系统间的通信，它是一个分层结构。

- 协议栈：建立并维护网络系统与被管元素间的通信链路，促使管理信息的正常传递。
- 报文拆装：实现管理报文与协议栈所支持的最大长度的报文间的匹配及转换，屏蔽不同网络环境对管理应用的影响。
- 报文格式转换：实现报文传输格式与网络管理系统内部报文处理格式间的转换。

(3) 管理信息通信服务(MICS)

管理信息通信服务提供网管系统元素的连通性。利用它作为下层结构可实现网管系统

中被管对象之间的相互通信。它可以分为以下几类：

- 管理信息服务：提供与被管对象进行交互的基础，这些交互包括报文读取、设置、删除、送达等。
- 应用实体通信服务：提供对管理进程内外对象的访问，可以透明地访问任意 MIB 中的对象。
- 进程间通信：利用计算机及网络操作系统的功能，提供管理进程间通信的能力和方式。

4. 网络管理功能间的关系

从 1.4 节可知，根据国际标准化组织的定义，一个专业的网络管理系统应包括配置管理、故障管理、性能管理、安全管理和计费管理 5 个方面的基本管理功能。

网络功能本身不是孤立的，完成一项网络管理功能往往也需要其他管理功能的配合，网络管理者、网络设备供应商、网络用户与网络管理功能之间有密切的关系。

(1) 故障管理与其他功能的关系

故障管理需要从性能管理得到当前的运行分析结果；从配置数据库得到设备配置信息。利用上述信息和网络的事故报告，一旦确认发生故障，通过配置管理来修改配置参数，启动恢复行动，修复、替换或隔离故障部件。将网络故障情况作为网络状态数据移交性能管理，以分析计算网络的可用性参数。故障处理结果将向网络管理者报告，有关用户也可以了解到故障发生的原因、处理结果以及应采取的措施或建议，如图 8-4 所示。

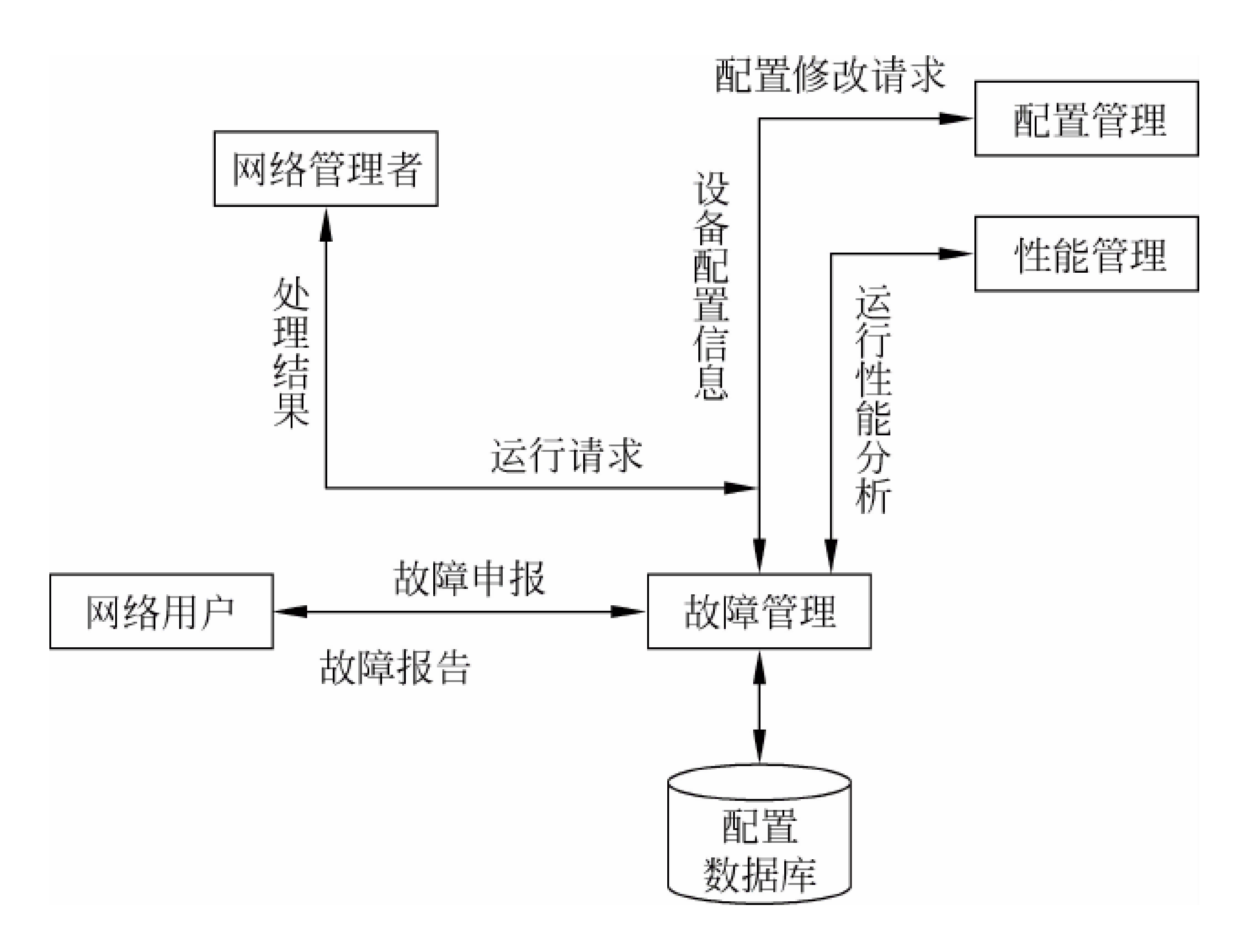


图 8-4　故障管理与其他功能的关系

(2) 配置管理与其他功能的关系

配置管理包括资源配置和业务配置两方面。资源配置通过资产管理从供应商那里得到硬件设备和软件版本，从性能管理和规划管理得到或增加网络资源请示，从故障管理获得为修复故障而重新配置资源的要求，从业务管理得到资源调整的请求，从配置数据库得到当前的资源配置。为实现新的资源配置，资源配置向资产管理申请额外的资源，如图 8-5 所示。

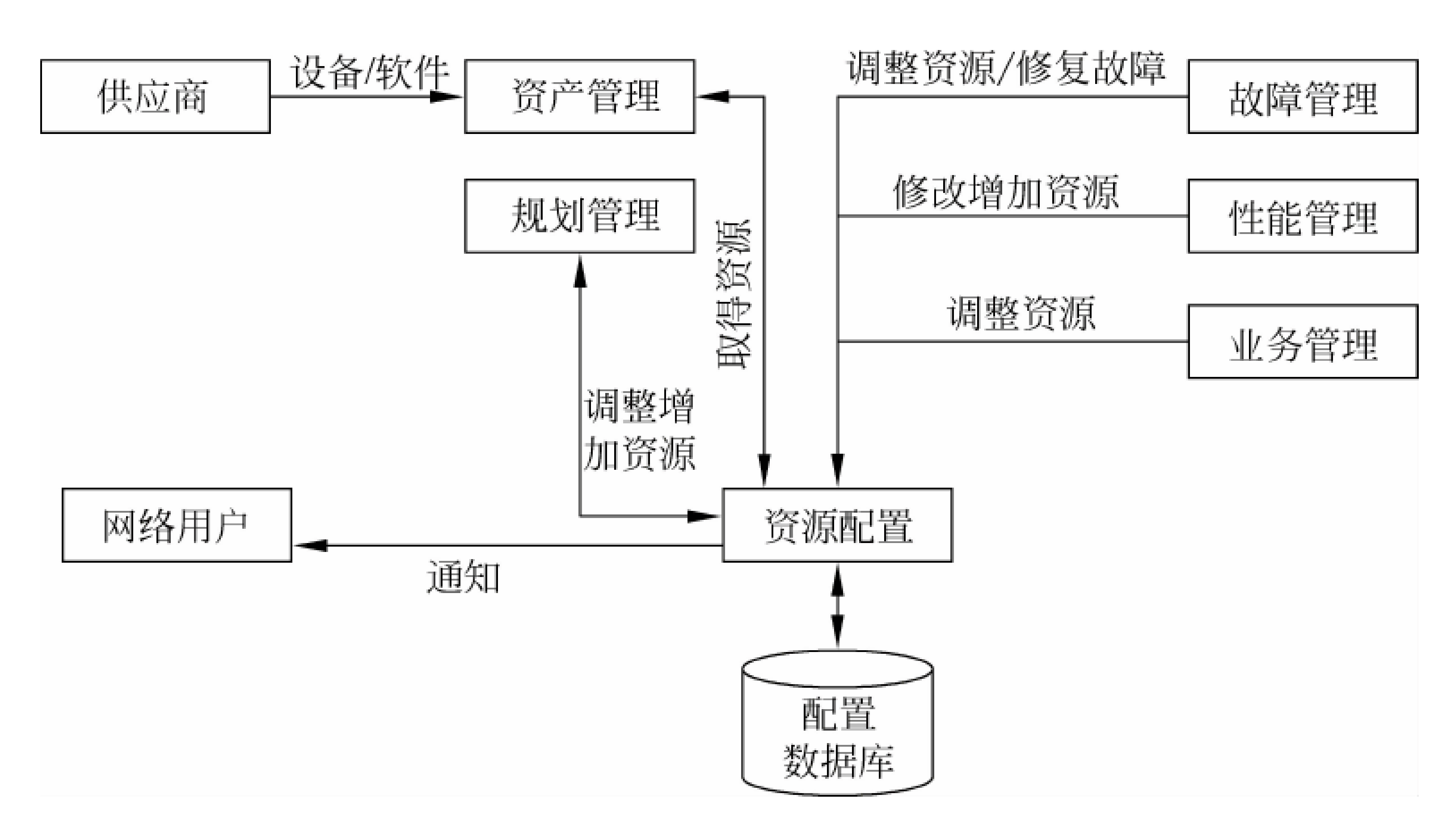


图 8-5　资源管理与其他功能的关系

业务配置从规划管理得到新的业务订单，从故障管理得到业务配置故障的通知，与网络用户协商配置业务。业务管理将通知计费管理对新的业务计费，通知故障管理对新配置的业务进行使用前的验证测试，业务配置把用户占用的设备设施和分担的成本情况反馈给资产管理，如图 8-6 所示。

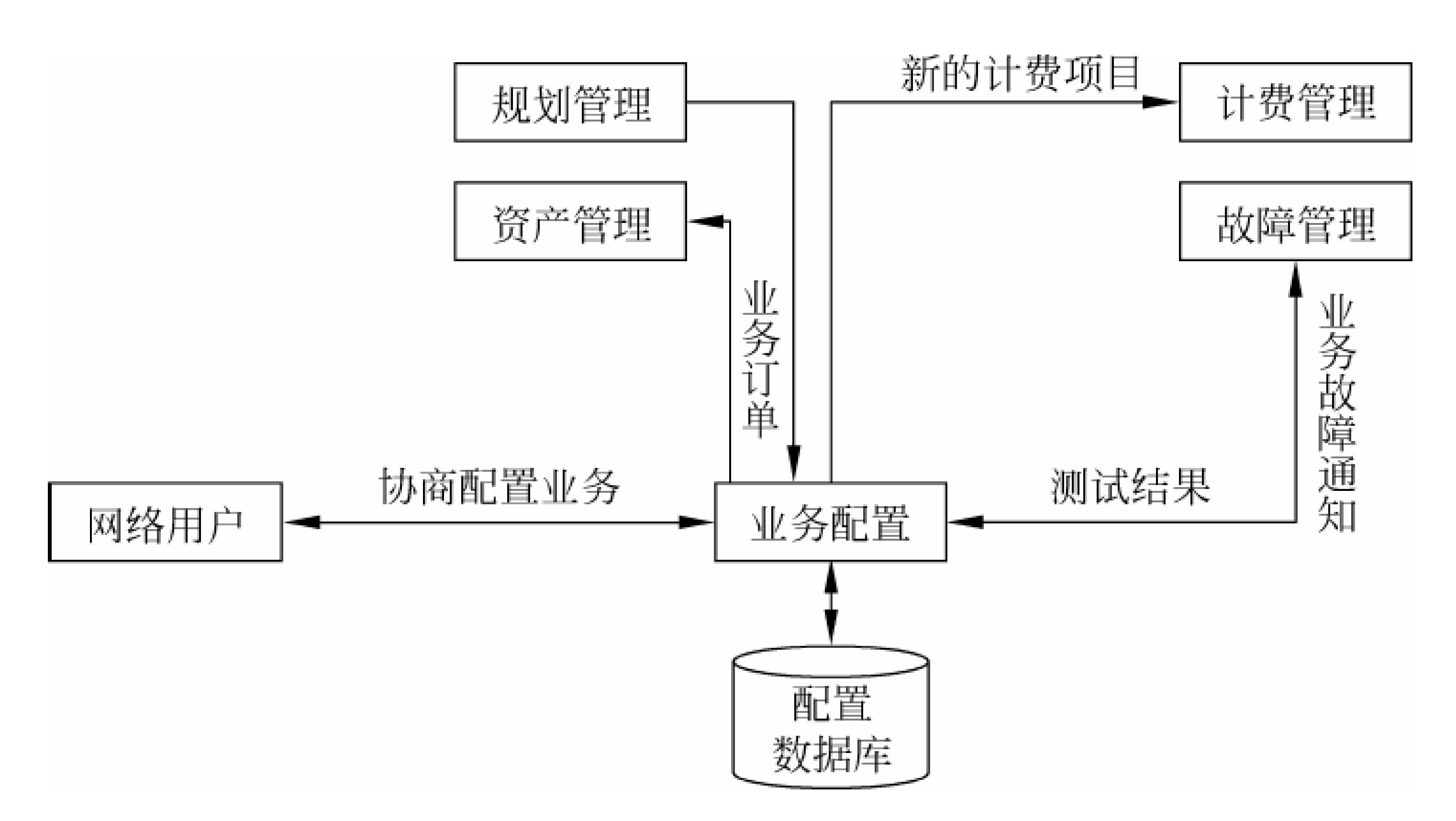


图 8-6　业务管理与其他功能的关系

(3) 性能管理与其他功能的关系

性能管理从网络管理机构获取当前网络运行的指标，从网络用户获取查询申请信息，从计费管理得到用户使用网络的详细记录，利用收集的统计数据和故障管理检测的可用性数据，计算网络性能参数。一旦出现危险状态则向故障管理示警。如果用户有查询的请求，则向用户反馈，并将运行性能的报告提交给网络管理机构。此外，规划管理从性能管理中获得运行的数据，能够实时了解网络的综合状况，以便有针对性地进行相应的调整和规划，如图 8-7 所示。

(4) 计费管理与其他功能的关系

计费管理从网络管理机构获得资费政策，从业务配置得到用户使用的业务情况，从资产管理得到用户占用的设备设施和分担的成本，从安全管理得到用户的预定义的文件，从网络

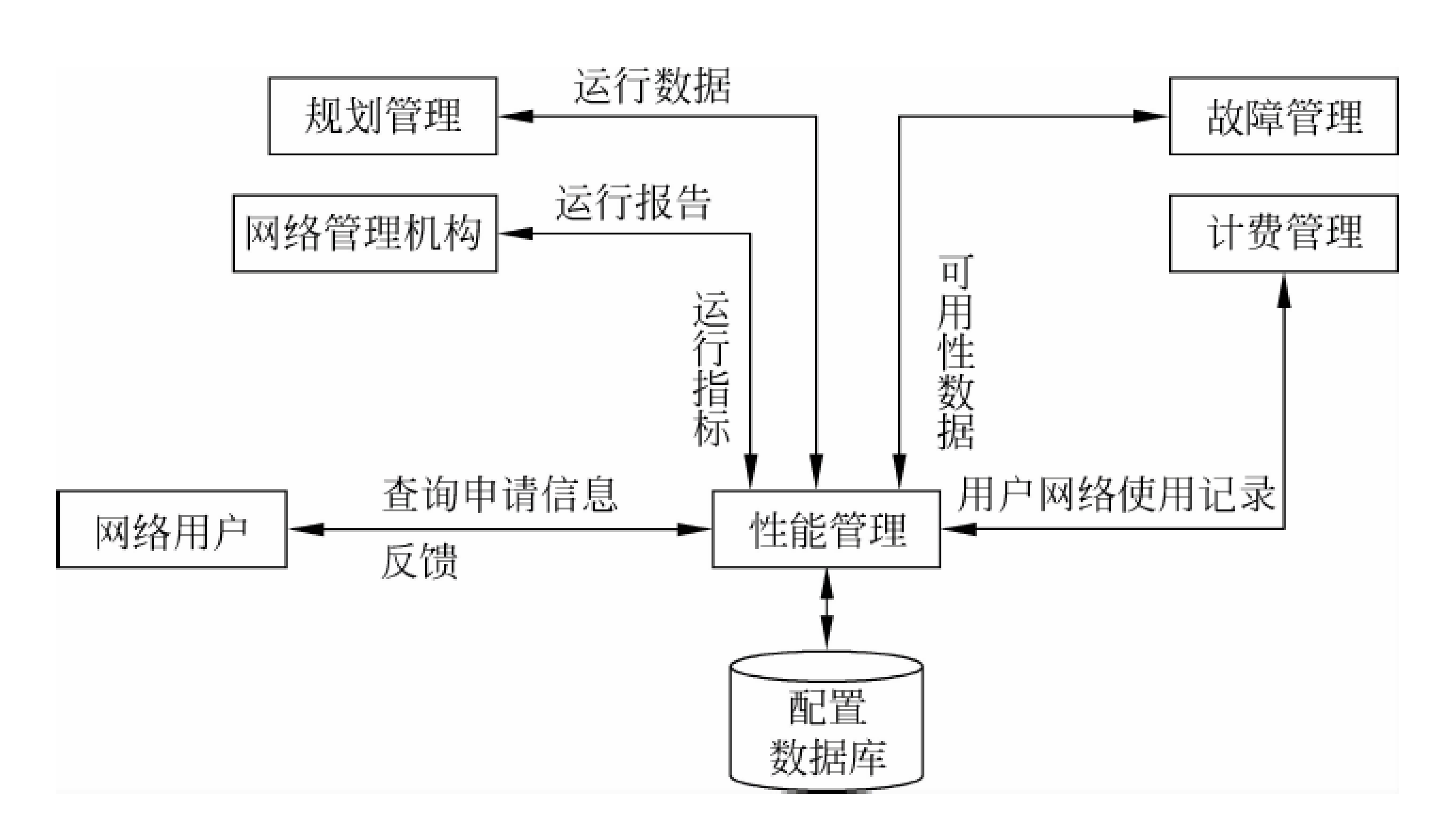


图 8-7　性能管理与其他功能的关系

用户得到查询请求，利用收集的计费记录，计算出每个用户的费用，然后将账单反馈给网络用户，如图 8-8 所示。

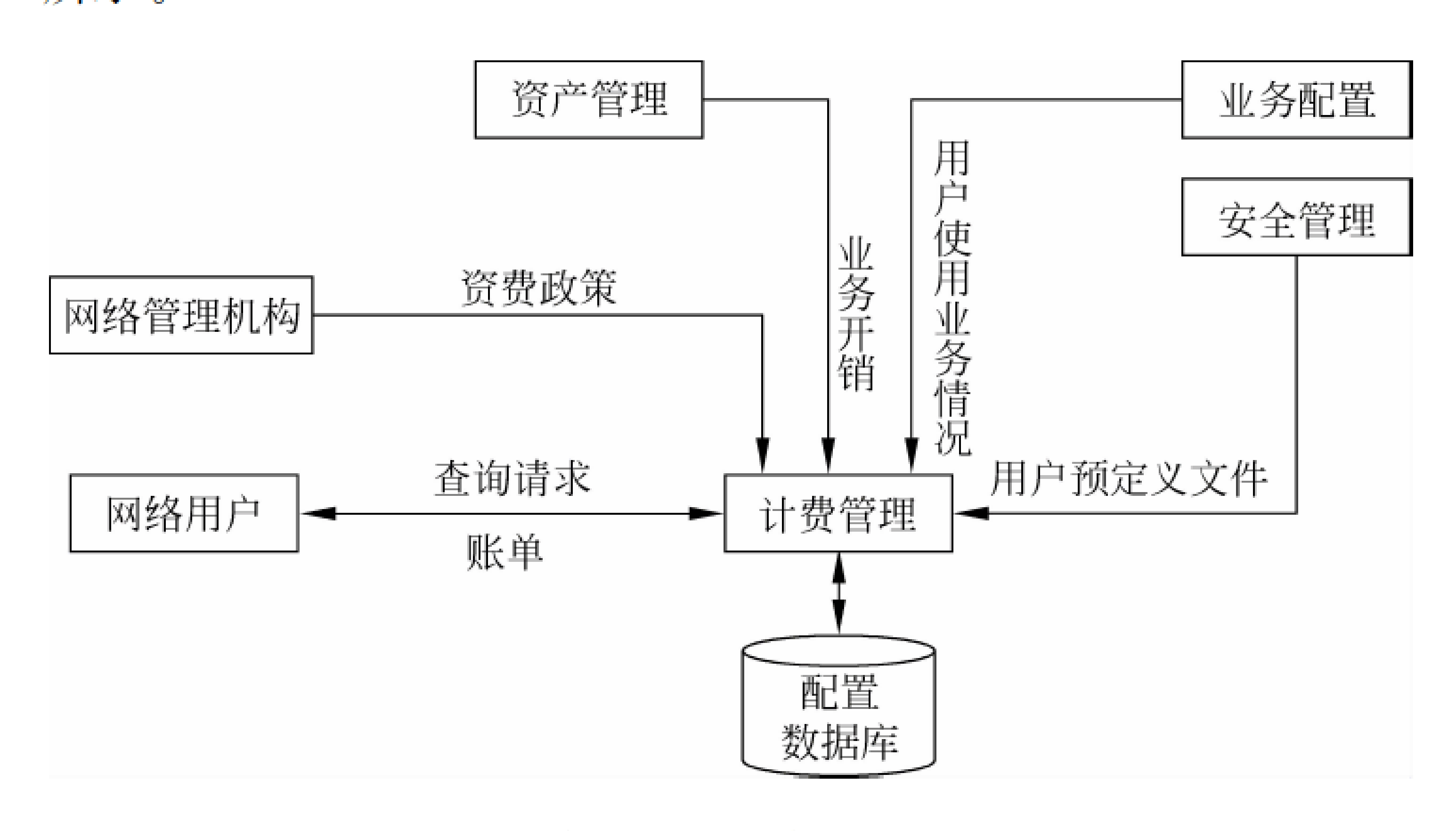


图 8-8　计费管理与其他功能的关系

(5) 安全管理与其他功能的关系

安全管理涉及网络的所有功能，是为实现安全目标而进行的有关决策、计划、组织和控制等方面的活动。运用现代安全管理原理、方法和手段，分析和研究各种不安全因素，从技术上、组织上和管理上采取有力的措施，解决和消除各种不安全因素，防止事故的发生。安全管理的主要任务是防止非法用户对资源的访问，安全管理与其他功能的关系如图 8-9 所示。

此外，规划管理、资产管理和人员管理也影响网络管理的五大功能。网络规划是将网络服务的商业策略转化为一套经济、有效的计划，去配置和拓展被管理的网络。网络规划管理就是建立网络的结构和配置，其结果直接影响着网络管理的其他功能，合理的规划有利于网络管理的进行，否则将影响网络正常、稳定、安全地运行。资产管理主要是指对网络有关设备、设施以及网络操作的人员进行登记、维护和查阅等一系列工作，资产管理是网络管理对象中的重要部分。人员管理也是网络管理系统的一部分，人是网络管理中的决定因素，网络规划、管理系统的设计、网络管理决策和操作等的结果都与管理人员的素质休戚相关。

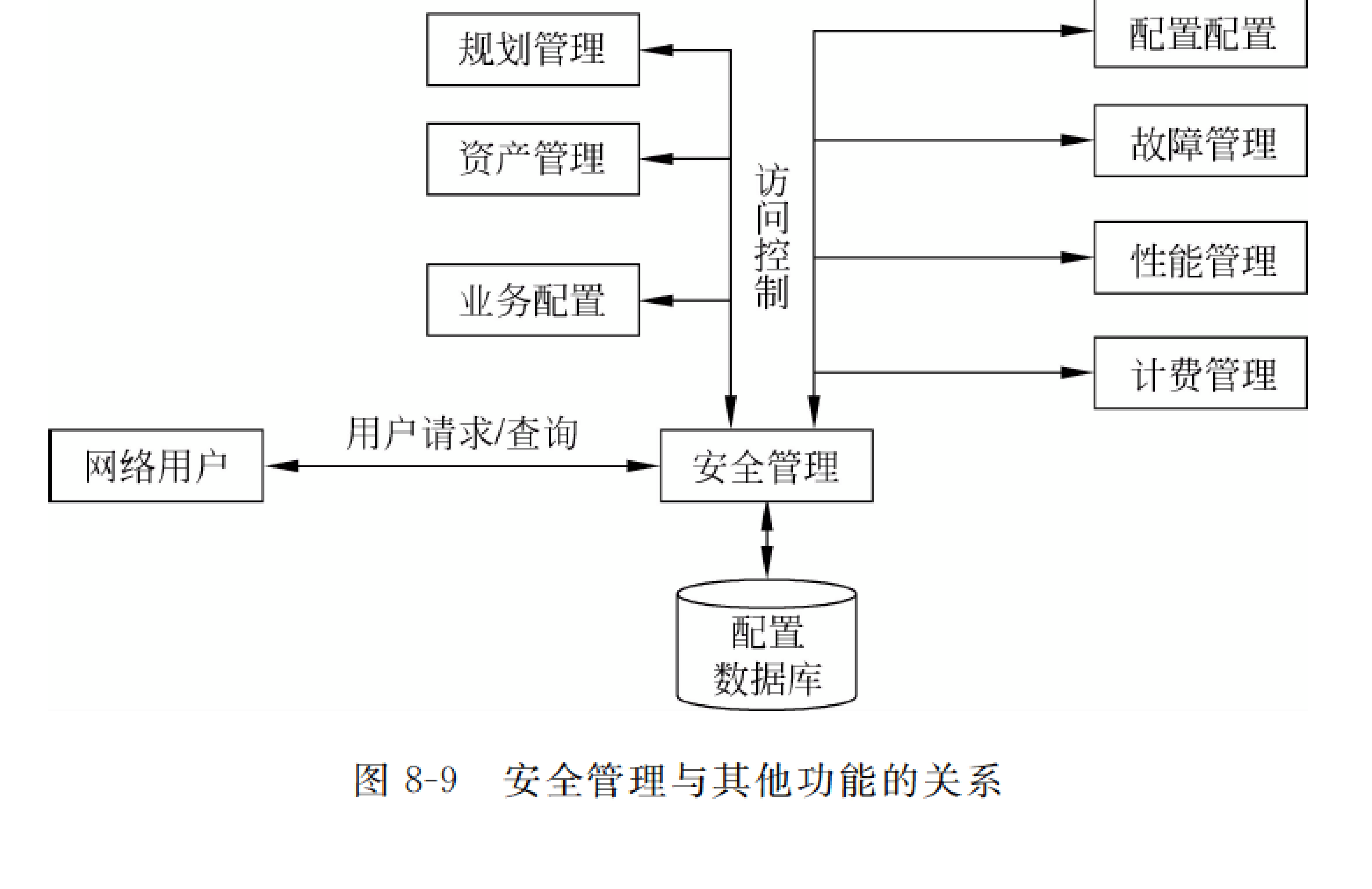


图 8-9　安全管理与其他功能的关系

8.2　常用网络管理工具

常用的网络管理工具有很多种，如链路测试、网络查看、网络诊断、服务器监控、设备管理、远程控制等工具。本节将介绍几种实用的管理工具。

8.2.1　服务器监控工具

1. 服务器监控工具的功能

服务器在运行的过程中可能会出现很多问题，如硬件损坏、软件没有运行、宕机等。更糟糕的情况是，服务器看似运行但实际上并没有履行“服务”的功能。一个企业所管理的服务器越多，出现问题的可能性就越大，服务器管理的难度也就越大。所以很好地监控服务器的运行状态是非常必要的。

监控工具所要监控的内容很多，总体可以分为三大块：监控服务器运行（运行状态）、监控服务器通信量（包括进和出）、监控服务器使用结果（日志、统计、分析）。服务器监控产品需要包含下列功能。

（1）物理硬件监控：即密切关注诸如硬盘等部件的温度、电源以及机能。所需监控的大都是相当关键的部件，它们一旦出现故障就意味着服务器死机。用于监控硬件的软件也都是特定的，如运行在 IBM 服务器上的软件可能就不能运行在 Dell 服务器上。

（2）服务器性能监控：即监控服务器的 CPU 使用率、可用磁盘空间、存储等，特别是在服务器很多的情况下，这既可以帮助发现并修理故障，也可以优化系统资源。

（3）服务监控：所有的服务器都运行着很多服务，其中很多对于服务器运行都是至关重要的，如果它们出现问题，那服务器也就没有作用了，所以很多监控软件专门提供类似服务。

（4）网络监控：服务器监控的很多领域都会与操作网络有关，所以网络监控也经常被认为是监控软件的单独一类。当然，很多通用服务器监控工具都包含有这样的功能。

总体来说，服务器监控软件种类很多，大多提供实时监控，显示服务器的当前状态，也提供服务器性能的历史监控记录。有的服务器监控工具被包含在一些大型服务器管理套件中，如 IBM Tivoli、CA Unicenter；也有独立的服务器监控工具，如 GFI 的 Server Monitor、

BMC 的 Server Monitoring and Management 等。

2. 服务器监控软件

NetFox 服务器监控软件实现了对网络及服务器故障的即时监控报警功能，监控结果可发送到手机，同时可接受手机发出的指令修复系统错误。使用该款软件可以在第一时间得知系统发生的异常，并可自动或通过手机遥控对异常进行处理。

NetFox 服务器监控软件能够实时监控 WWW 服务、FTP 服务、Mail 服务、网卡、网关、CPU 资源占用率、内存使用率、硬盘空间、ping 响应、服务器心跳、文件状态等，当检测值达到用户设定的报警阈值时启动多种预制报警方式进行报警，具有完善的设定、搜索、日志、报表及打印功能，适用于各种工业、商业、政府、教育、传媒等领域使用。配合 NetFox 服务器监控仪硬件，可实现更多实用功能，其工作界面的"系统设置模块"如图 8-10 所示。



图 8-10 NetFox 服务器监控软件

3. 服务器监控网站

服务器监控网站有 HyperSpin (http://www. hyperspin. com)、Dotcom-Monitor (http://www. dotcom-monitor. com)、网站保姆(http://bm. chinaz. com)、Uptime. com. cn (http://www. uptime. com. cn)、host-tracker(http://host-tracker. com)、Gomez(http://www. gomez. com)、Site24×7(http://www. site24x7. com)、SiteUptime(http://www. siteuptime. com)等。以 HyperSpin 网站为例，该网站的功能如下：

- 24×7×365 全年不间断监测站点是否正常运行。
- 支持多种通信协议；支持 ping、HTTP、HTTPS、FTP、SSH、SMTP、DNS、POP3、IMAP、MySQL 和其他标准的 TCP/IP 应用服务。
- 具有停机通知功能，一旦站点或服务器不能访问，会第一时间通过电子邮件与手机短信通知。
- 全球多个监测基点，可对站点在全球范围内进行监测，不仅监测站点是否在运行，而且还能检测来自全球各地的客户能否访问站点。
- 提供实时运行状态报告。
- 当服务器停机时，可自动发出请求重启或其他要求的电子邮件。

• 在线时间与性能报告。
• 尽量减少虚报，聘请高级工程师为客户核实真伪警报。
• 计划监测任务。用户可以设置(一次性或循环多次)维护计划。
• 免费整合数据，如有使用其他的监测服务，可以导入到客户新的账户里。

HyperSpin 首页如图 8-11 所示，这里输入的是新浪的网址，单击“监测”按钮即可进行监测。



图 8-11 HyperSpin 网站主页面

监测的结果如图 8-12 所示。

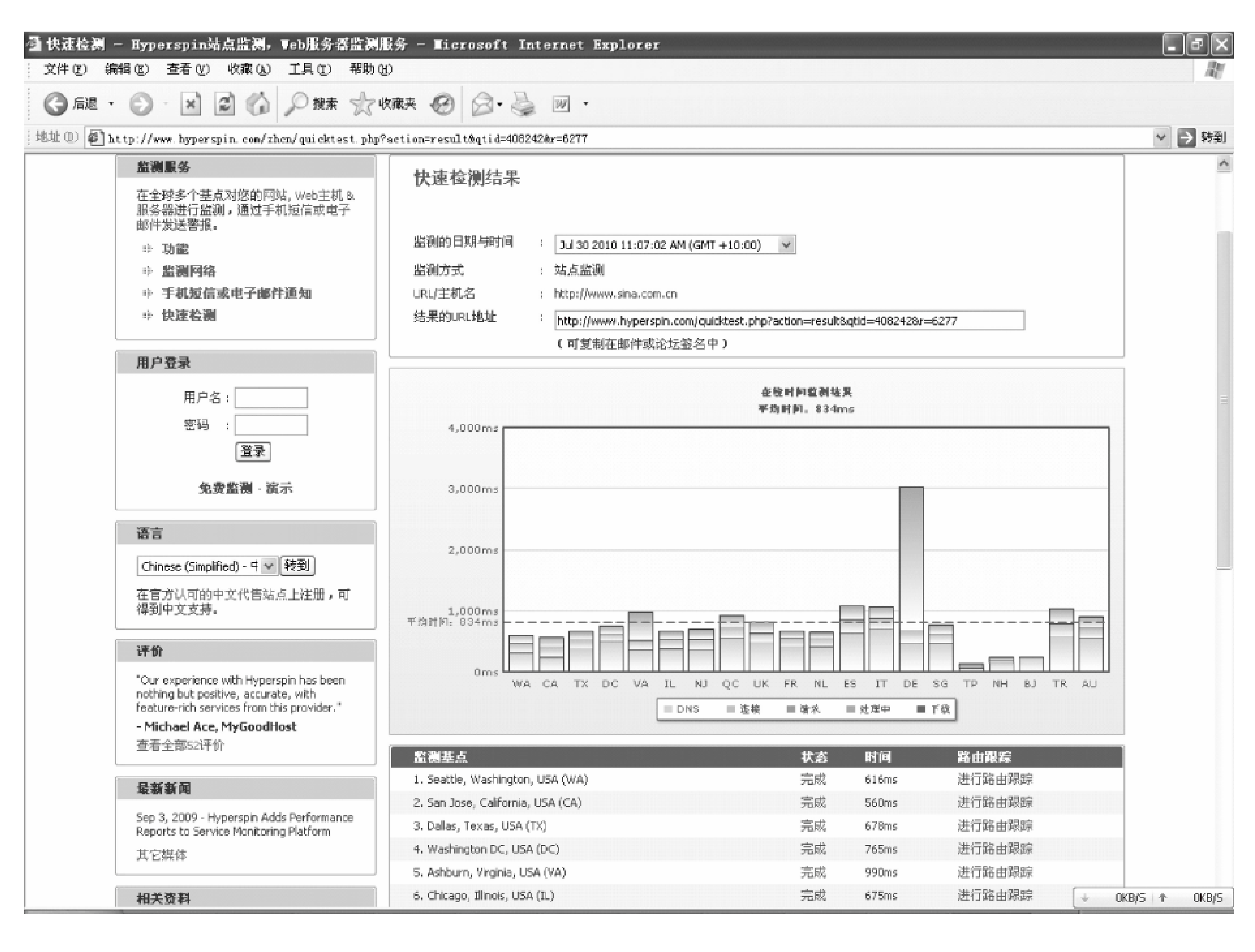


图 8-12 HyperSpin 网站测试结果页面

8.2.2 网络性能监控工具

网络性能决定着网络服务的质量，因此对响应时间、网络延迟、延迟变化、吞吐量、链路利用率、资源利用率、丢包率、可用性和可靠性等网络性能指标的监控具有非常重要的现实意义。对网络性能进行测量、分析、评价、控制和调整，有利于对网络运行状况进行实时监测、有利于网络的进一步合理规划和优化等。下面以吞吐量测试工具 QCheck 3.0 为例说明网络性能监控的方法。

网络性能不仅与交换和路由设备的性能相关，而且与线路质量也有很大关系，使用 QCheck 可以测试网络性能。QCheck 是一款免费网络测试软件，主要功能是向 TCP、UDP、IPX、SPX 网络发送数据流来测试网络的吞吐率、回应时间等，从而测试网络的响应时间和数据传输率。

测试时需要使用两台计算机，并且均需运行 QCheck 软件。在测试中，从一个客户端向另一个客户端发送文件，然后测试所消耗的时间，并计算出传输速率(以 Mbps 为单位)。例如 TCP/UDP 传输率测试，测试结果越高越好，100Mbps 端口的理论值最高为 94Mbps(传输率)。

1. 运行 QCheck

在要测试的网络两端分别运行一台计算机，这两台计算机均安装 QCheck 软件，然后分别运行 QCheck 程序，如图 8-13 所示为 QCheck 主界面。

在 QCheck 界面上方，"From Endpoint 1"表示要发送数据的节点；"To Endpoint 2"表示要将数据发送到的节点。下方有几个圆形按钮，左侧"Protocol"内的绿色按钮表示可以使用的协议类型，包括 TCP、UDP、SPX 和 IPX。右侧"Options"内的棕色按钮表示可以测试的项目，并且不同的项目适用于不同的协议：

- Response Time(响应时间)可以测试响应的最短、平均与最长时间，该测试适用于所有协议。
- Throughput(吞吐量)用来测试每秒发送的数据量，以测试网络带宽。该测试适用于所有协议。
- Streaming(流)用来测试串流传输速率，如多媒体流的带宽，该测试只适用于 UDP 和 IPX 协议。

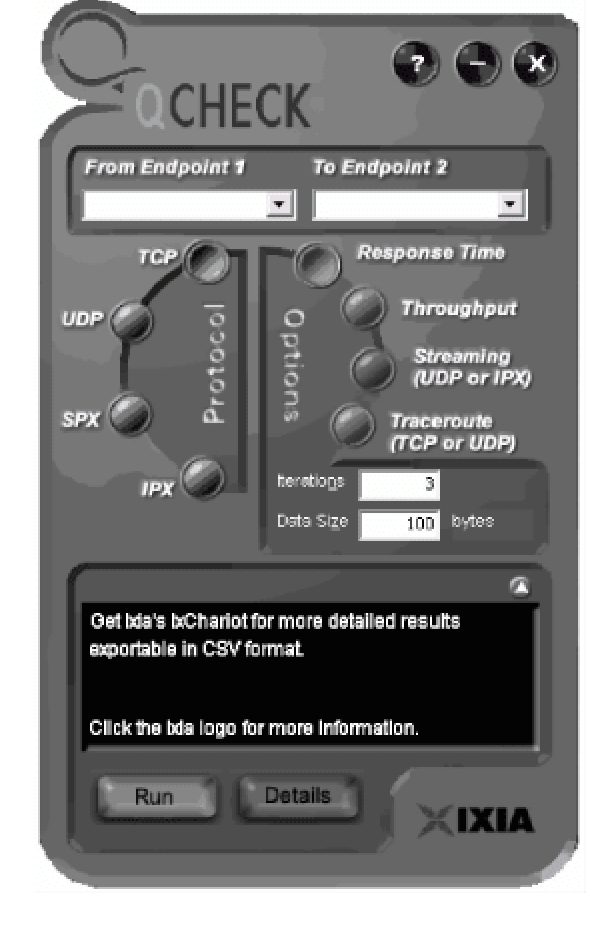


图 8-13 QCheck 主界面

- Traceroute(路由追踪)相当于 Windows 中的 Tracert 命令，用来测试一台计算机到另一台计算机所经过的路由，该测试只适用于 TCP 和 UDP 协议。

在进行测试时，首先需要单击左侧相应的按钮来选择要测试的协议，然后在右侧单击选中所要使用的测试类型，再单击 Run 按钮即可开始测试，测试完成以后会在下面的黑色框中显示测试结果，并可以单击 Details 按钮查看详细信息。

2. 测试 TCP 响应时间

TCP 响应时间测试可以测得完成 TCP 通信的最短、平均与最长时间。这个测试类似于 ping 命令，可以让用户知道到达另一台计算机所需要的时间。这个测量一般称为"延缓"或者"延迟"。

在 QCheck 主界面中，在 From Endpoint 1 下拉列表框中选择 localhost 选项，表示从本地计算机发送测试，在 To Endpoint 2 下拉列表框中输入目标计算机 IP 地址；在 Protocol 中单击选中 TCP 按钮，在 Options 中单击选中 Response Time 按钮；在 Iterations 文本框中输入重复测试的次数，默认为 3 次；在 Data Size 文本框中输入要发送的数据包的大小，默认为 100 bytes。完成后单击 Run 按钮，QCheck 便开始测试，测试完成后，在 Response Time Results 文本框中显示出测试结果，如 Minimum、Average 与 Maximum 时间，如图 8-14 所示。

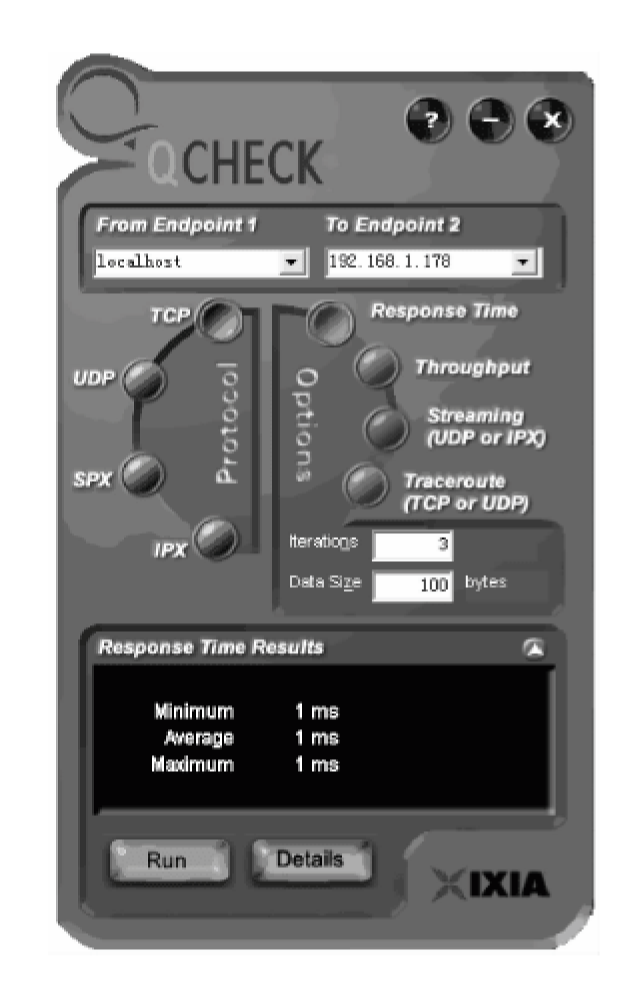


图 8-14　测试 TCP 响应时间

如果想查看更详细的信息，可以单击 Details 按钮，打开 QCheck Results 窗口，如图 8-15 所示，该窗口中显示了设置信息、测试结果、本地计算机与目标计算机的系统信息以及 QCheck 的版本信息等。

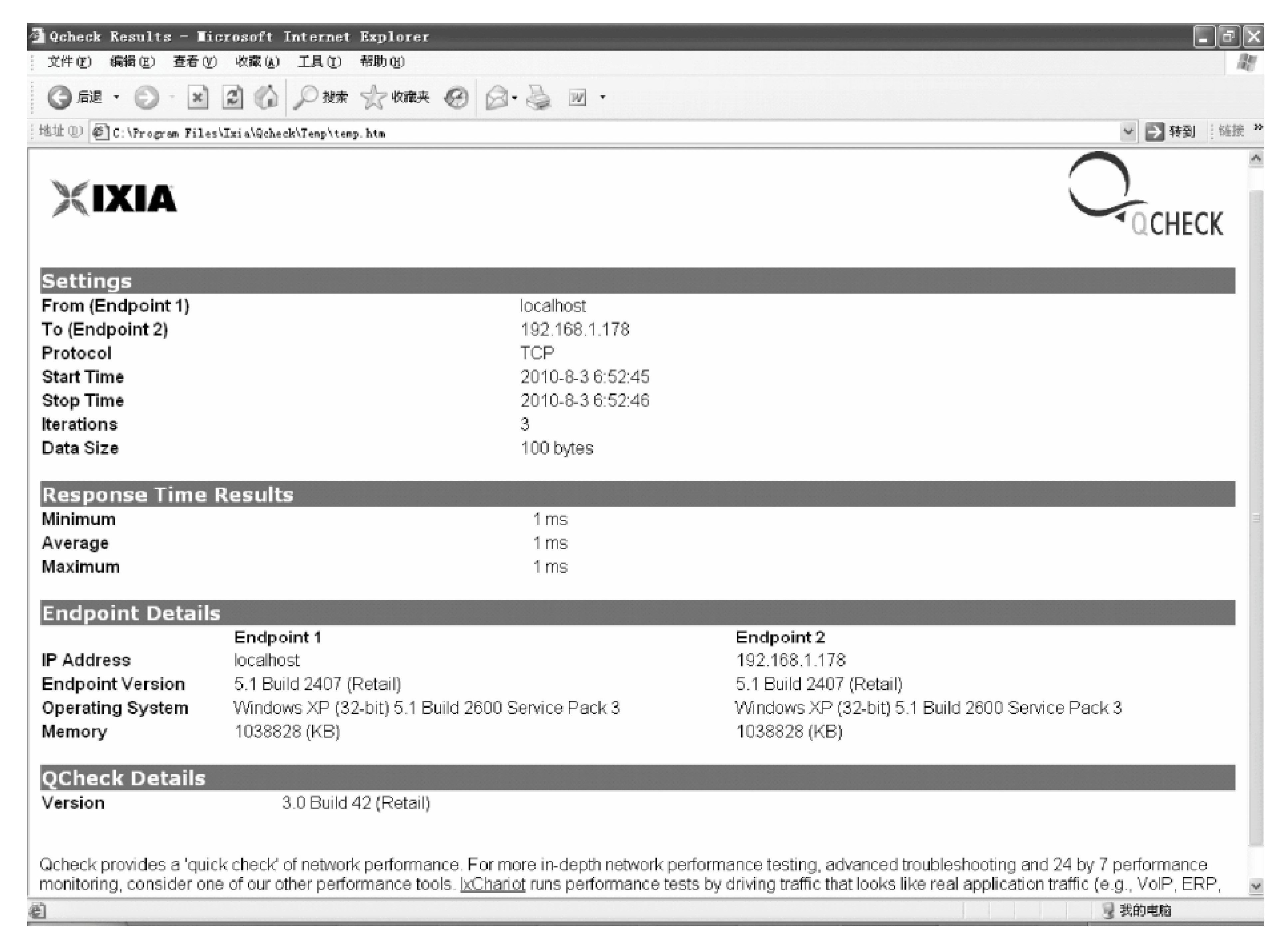


图 8-15　QCheck Results

3. 测试网络带宽

要测试从本地计算机到目标计算机之间的网络带宽，可以使用 TCP Throughput 测试，这项测试可以测量出两个节点间使用 TCP 协议时，每秒钟成功发送的数据量。

在 QCheck 窗口中，在 From Endpoint 1 下拉列表框中选择 localhost，在 To Endpoint 2 下拉列表框中输入目标计算机的 IP 地址；在 Protocol 中单击 TCP 按钮，在 Options 中单击 Throughput 按钮；在 Data Size 文本框中可设置要发送的数据包的大小，默认为 100KB，这里，设置为 1000KB。设置完成后单击 Run 按钮，QCheck 开始测试，测试完成后在

Throughput Results 文本框中显示出测试结果，如图 8-16 所示。这里，测试出的 Throughput 为 800.008Mbps，也就是说，从本地计算机到目标计算机的带宽为 800.008Mbps。

在测试网络带宽时，往往会因为设备性能、线路质量等各种因素的影响，而使得测试值比实际值要小。因此，为了求得准备的结果，建议使用多台计算机进行测试，一般最大值才是网络带宽的真实值。

4. 串流测试

使用 QCheck 的 UDP 串流传输率测试，可以测试多媒体流需要多少频宽，以方便网络硬件速度和网络所能达到的真正数据传输率之间的比较。

和多媒体应用一样，串流测试会在无连接的状况下传送数据。在 QCheck 中，使用无连接协议的 IPX 或者 UDP。QCheck 的串流测试是评估应用程序使用串流格式时的表现，例如 IP 线上语音以及视频广播。

在 QCheck 主界面中，在 From Endpoint 1 下拉列表框中选中 localhost 选项，表示从本地计算机发送测试，在 To Endpoint 2 下拉列表框中输入目标计算机 IP 地址，在 Protocol 中单击选中 UDP 按钮，在 Options 中单击选中 Streaming 按钮；在 Data Rate 文本框设置数据传输速度，默认为 50kbps，最大不能超过 1Mbps；在 Duration 文本框中设置持续时间，默认为 10s。设置完成后，单击 Run 按钮，QCheck 开始测试，测试完成以后便会在 Streaming Results 文本框中显示，如图 8-17 所示。

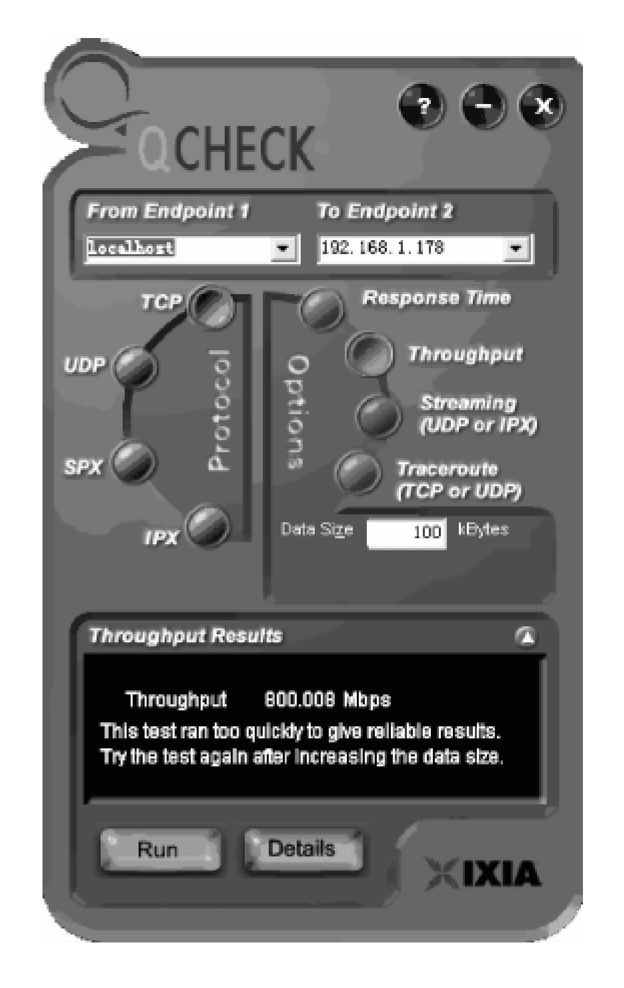


图 8-16　测试网络带宽



图 8-17　串流测试

8.2.3　网络流量监控工具

网络流量监控工具有很多，如 Bandwidth Meter Pro、Net Meter、DU Meter、NetLimiter 2 Monitor 等。下面以 Bandwidth Meter Pro(http://www.bandwidth-meter.net)为例进行介绍。

Bandwidth Meter Pro 可以监视带宽的使用情况，并且可以为一个或者更多所选择的网络连接显示实时的统计图表。该软件还可以生成每天、每周和每月的报告，详细列记带有累计带宽消费量的上传和下载使用情况。该软件还包括一个当在最后若干秒之内下载的字节少于若干字节的情况下发出通知的选项，以及一个简单的连接职守和用于导出报表为

.txt、.csv 和 HTML 等格式的选项。工作主界面如图 8-18 所示，可以通过不同的图像形式观察上传和下载的实时速率。

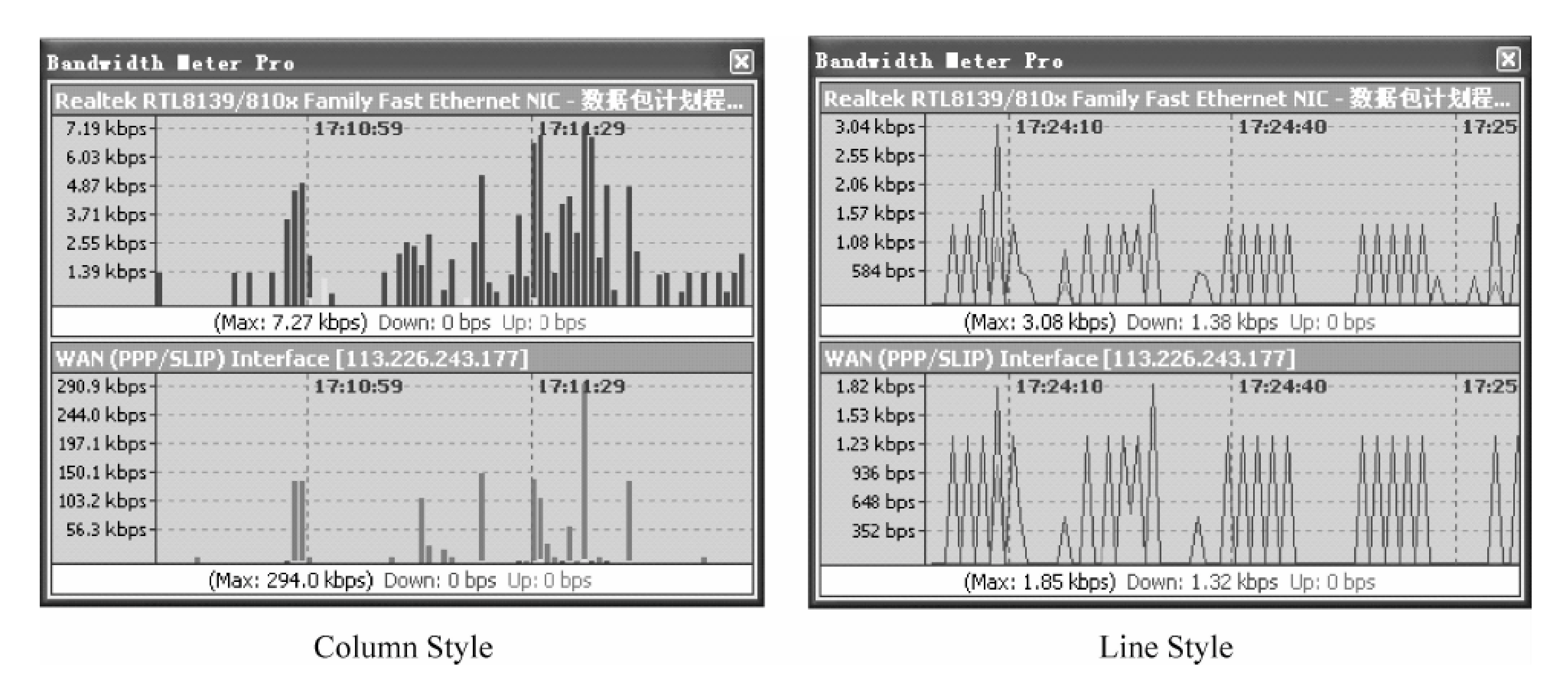


图 8-18　Bandwidth Meter Pro 流量监控主窗口

1. 配置界面

如图 8-19 所示，在主窗口中单击鼠标右键，并从快捷菜单中选择适视图（View），接着可以继续进一步选择其他项目进行相应的操作。

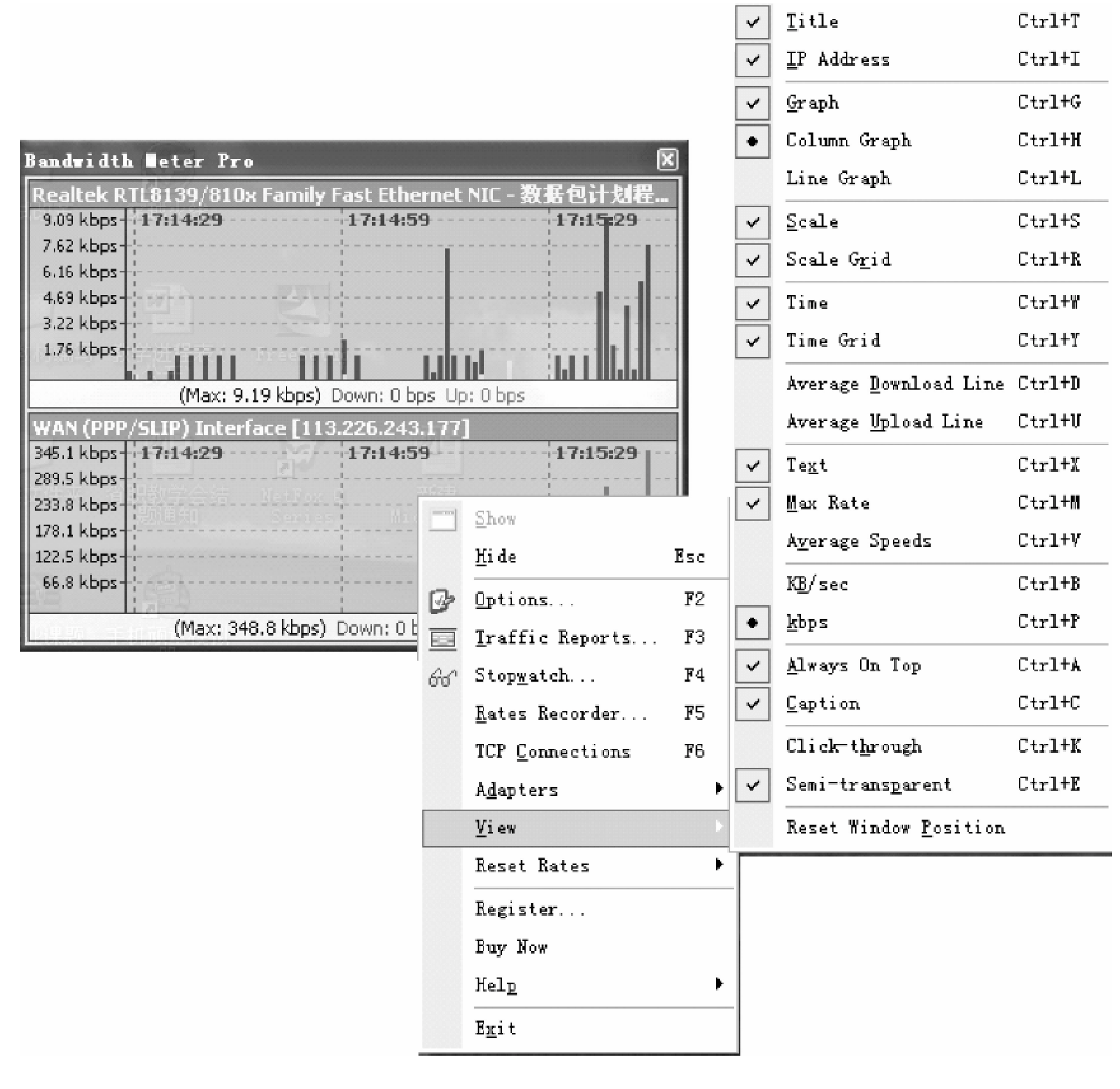


图 8-19　配置界面示意图

2. 适配器选择

如图 8-20 所示，在主窗口中单击鼠标右键，从快捷菜单中选择适配器(Adapters)，然后选择/不选任一适配器。Bandwidth Meter Pro 同时可以监视多个适配器。

图 8-20 适配器选择示意图

3. 带宽使用通知

如图 8-21 所示，当带宽超过预设的值时，可以用声音、音乐、E-mail 和运行特定程序的形式通知用户。

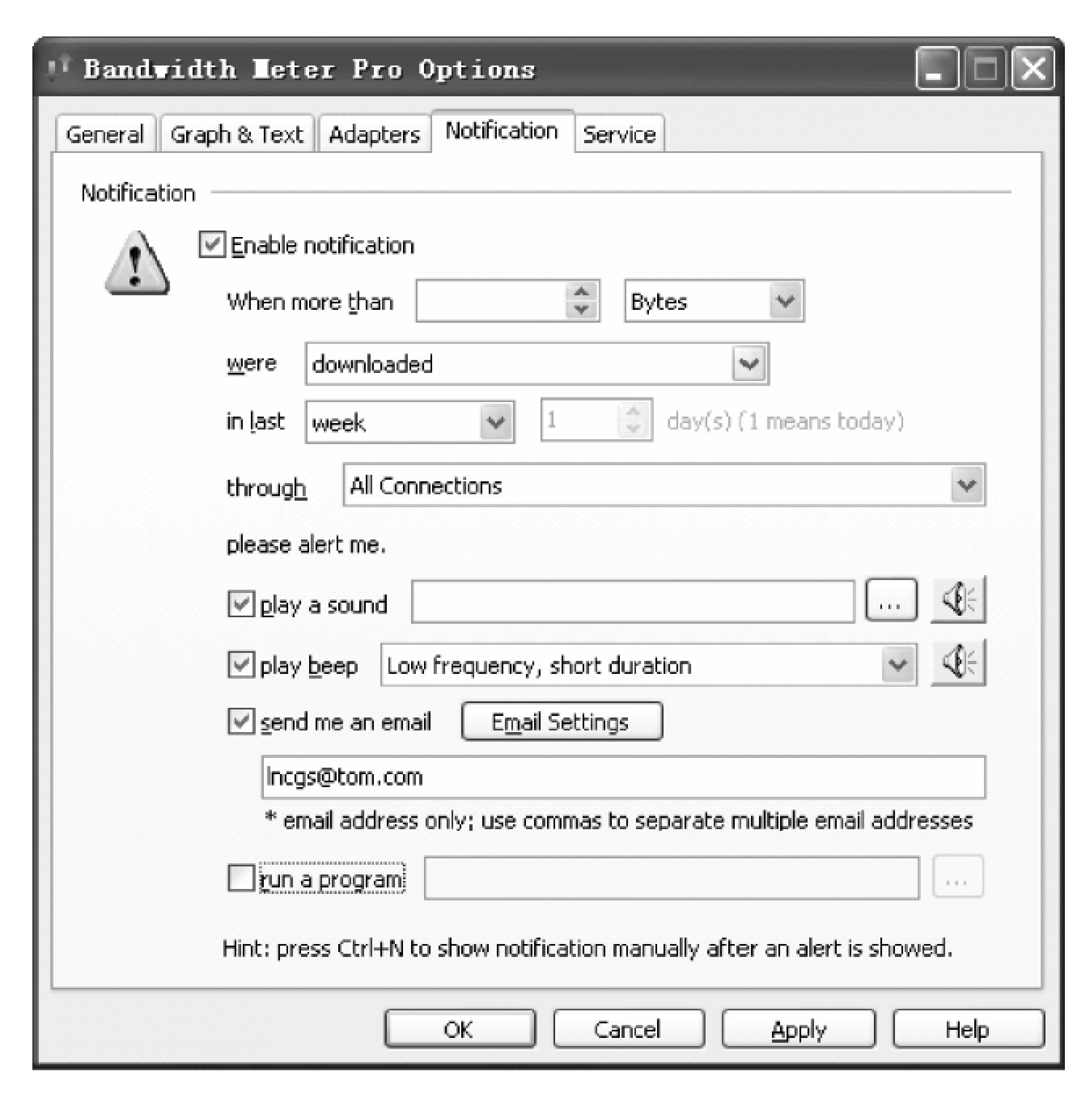


图 8-21 带宽使用通知设置

4. 流量报告

在主窗口中单击鼠标右键，并从快捷菜单中选择流量报告(Traffic Reports)，然后可以查看流量的概要情况，以及每天、每周和每月的流量报告，如图 8-22 所示。

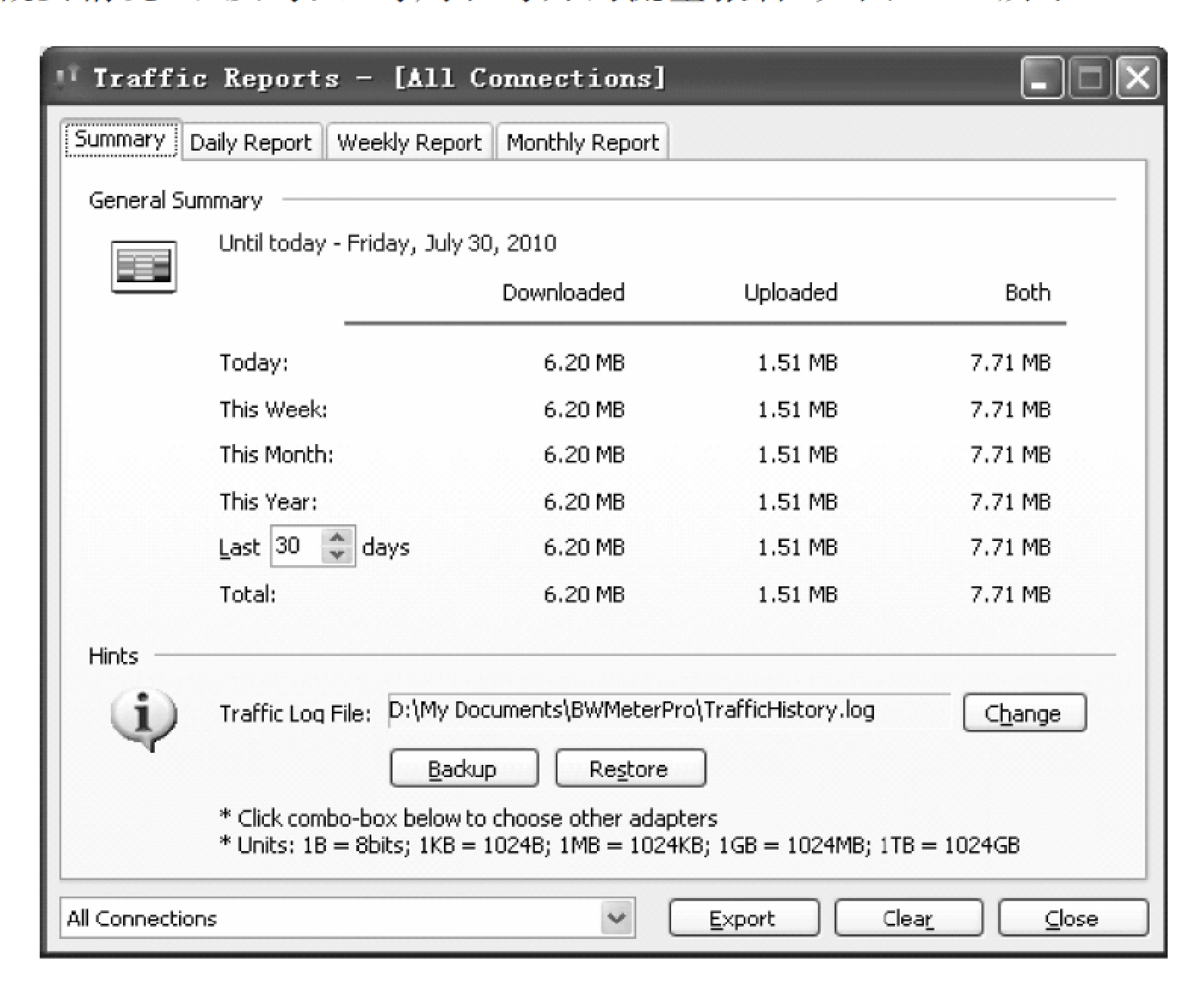


图 8-22 流量概要情况

8.3 企业级网络管理系统

目前市场上网络管理系统软件有不少，但真正具有网络管理五大功能的网络管理系统却不多。比较不错的网络管理系统有 HP 公司的 Open-View、IBM 的 NetView、SUN 的 SunNet、Cabletron 的 SPECTRUM，以及国内的 SiteView、网强等。

8.3.1 SiteView ECC

1. SiteView ECC 简介

SiteView ECC 是北京游龙网络科技有限公司的网络管理产品，专注于对局域网、广域网和互联网上的系统应用、服务器和网络设备的故障监测和性能管理，是集中式、跨平台的系统管理软件。SiteView ECC 通过持续监控企业 Internet、WAN、LAN 上的服务器、网络设备和应用系统的运行状况，可以对中间件、数据库、邮件系统、DNS 系统、FTP 系统、OA 系统、ERP 系统等进行全面深入的监测，从而确保企业信息平台全天候高效稳定地运行，其系统架构如图 8-23 所示。

SiteView ECC 功能强大，不仅方便系统管理人员随时了解整个 IT 系统的运行状况，而且能从应用层面对企业 IT 系统的关键应用进行实时监测。一旦系统出现异常，警报系统将通过声音、E-mail、手机短信息和脚本等方式及时通知相关人员；对于一些常见问题，SiteView ECC 还可以自动进行故障处理。SiteView ECC 完善的性能分析报告能帮助系统管理人员及时预测、发现性能瓶颈，同时为企业系统的战略规划提供依据。

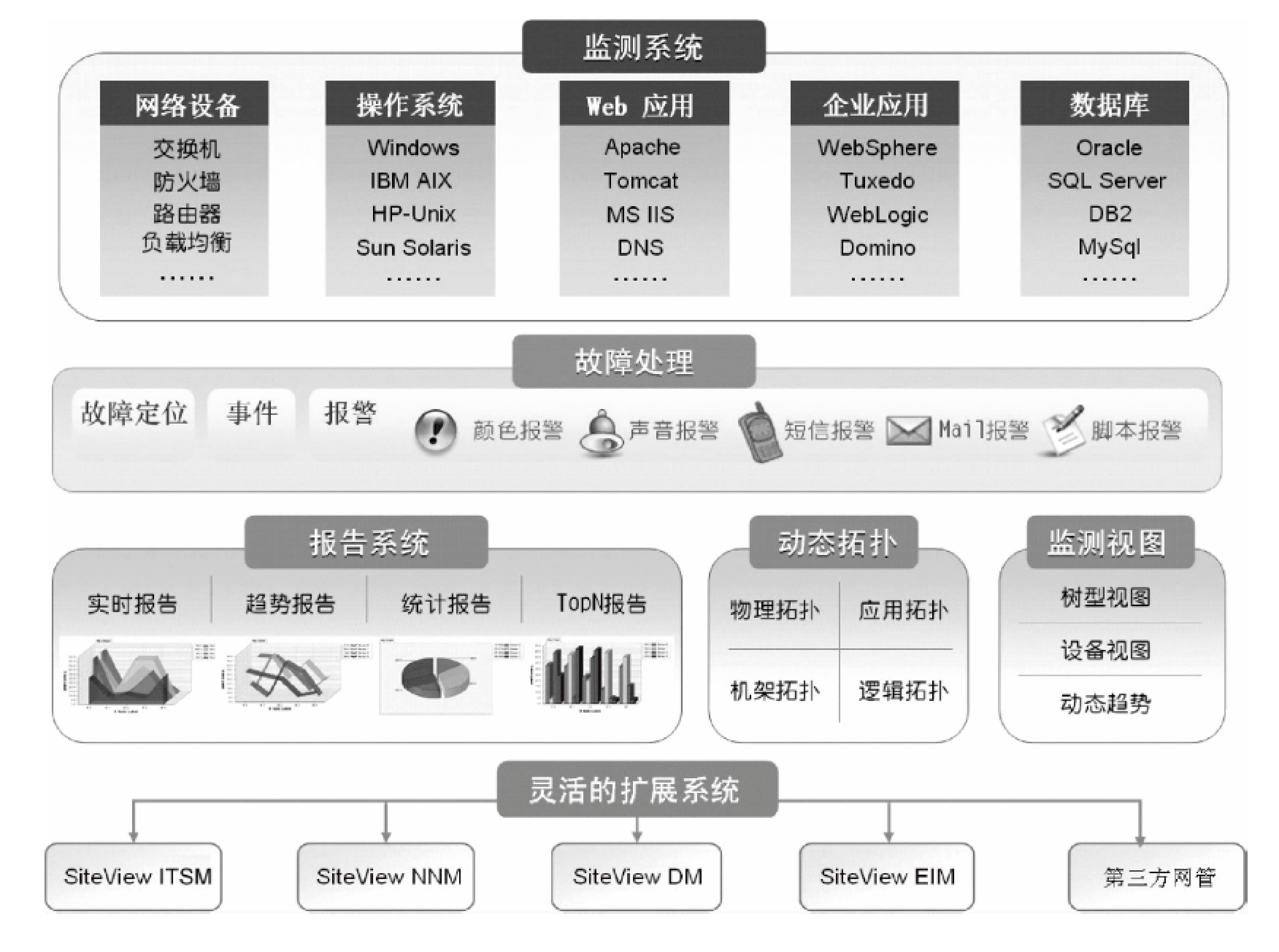


图 8-23　SiteView ECC 系统架构图

SiteView ECC 可以和 SiteView 系列产品——网络设备管理、上网行为管理、网络流量分析、网络流量控制、桌面管理无缝集成，为用户提供灵活的随需应变解决方案。

2. SiteView ECC 的功能

(1) 驾驭综合系统管理

专注对局域网、广域网和互联网上的网络基础架构、应用系统、数据库、中间件的故障监测和性能管理，全面解决在日常 IT 管理中遇到的问题。

(2) 实现全面深度监测

内置上千种各类专门的监测器，采用插件外挂方式与系统集成，用户还能通过 MSL 语言快速开发自己应用系统专门的监测器，实现无所不能的监测。

(3) 完美呈现拓扑视图

通过与 Visio 的完美结合，既可反映服务器、网络设备等网络基础架构的连通状况，也可反映应用流、数据库、中间件的运行情况。表现力极其丰富，多层次的网络拓扑图可很好地满足不同层面管理人员直观了解系统运行状况的需求。

(4) 报警及时，报告丰富

及时提供短信、邮件、声音、脚本等警报方式，并能根据用户需求自动生成各种美观的图形、图表分析报告。

(5)为 IT 系统管理部门服务

为 IT 系统管理部门提供真正集中式的远程管理工具，IT 系统的任何异动尽在掌握之中，使 IT 服务管理不再遥远。

3. SiteView ECC 的基本管理功能

1) 组管理

SiteView ECC 软件可以设置上千个监测，所以很有必要对这些监测进行分组管理。通

过监测的分组管理功能，用户可以更加直观、方便地了解各监测的状态和系统性能。

系统提供了二层交换机、三层交换机、路由器、防火墙、服务器、PC 设备、其他设备七个默认的组。用户可以将自己的设备添加到这些默认组里面，进行分类和管理；也可以任意增加子组按自己的方式进行分类和管理。增加子组操作过程如下：

在 SiteView ECC 左侧功能导航"监控器"中单击"整体视图"，然后在显示的页面中单击"增加子组"，其中：

- 依靠关系　此功能用于选择一个被当前组依靠的监测器，当前组内各监测是否运行将依靠于选定监测器的状态，默认为无依靠。
- 依靠条件　依靠条件分为三种：正常、危险、错误。如果选择"正常"，则只有当依靠监测的状态是正常时，本组内各监测器才会运行；如果选择"危险"，则只有当依靠监测的状态是危险时，本组内各监测器才会运行；如果选择"错误"，则只有当依靠监测的状态是错误时，本组内各监测器才会运行。

此外，还可以对组进行编辑、删除、禁止监测、启用监测等操作。

2）设备管理

SiteView ECC 监测设备指在监测网络内，被纳入 SiteView ECC 系统监测范围内的设备，包括服务器、路由器、交换机、防火墙等。在监测各项设备之前，必须在设备列表页面选择相应类型下要添加的设备，设备信息输入完毕后保存，这样设备就添加成功了，可以批量添加监测器，实现对该设备的监测。添加设备的操作方法如下：

（1）在 SiteView ECC 左侧功能导航"监控器"中单击"整体视图"，然后在显示的页面中单击"添加设备"选项，在设备列表中列出了可供选择的设备，包括添加服务器，网络设备，数据库，URL，防火墙，中间件，邮件服务，负载均衡，应用系统，DNS。

（2）以添加 Windows 服务器为例。右击 SiteView ECC，选中"添加设备"选项，在弹出的设备列表页面中选择"Windows 设备"，在"添加 Windows 服务器"对话框中输入相应的信息，输入完成后单击"保存"按钮，就完成了对 Windows 服务器的添加，如图 8-24 所示。



图 8-24　添加设备对话框

设备添加成功后，新添加的设备将会出现在树形结构的最下方和设备列表的最下方。

3）监测器管理

SiteView ECC 软件包括很多的监测器，同一类的监测器放在相应的设备里面，不仅提供了单个监测器添加功能，还提供了批量监测器添加功能，下面就简单介绍一下对监测器的具体操作。

（1）增加监测器

在控制台树中单击需要添加监测器的设备名称，进入该设备的详细页面。在该页面中，单击"添加监测器"，可看到该设备下可添加的监测器的列表，如图 8-25 所示。

Windows 设备提供了 14 个监测器，分别是：Ping、Port、URL、CPU、Disk、Memory、

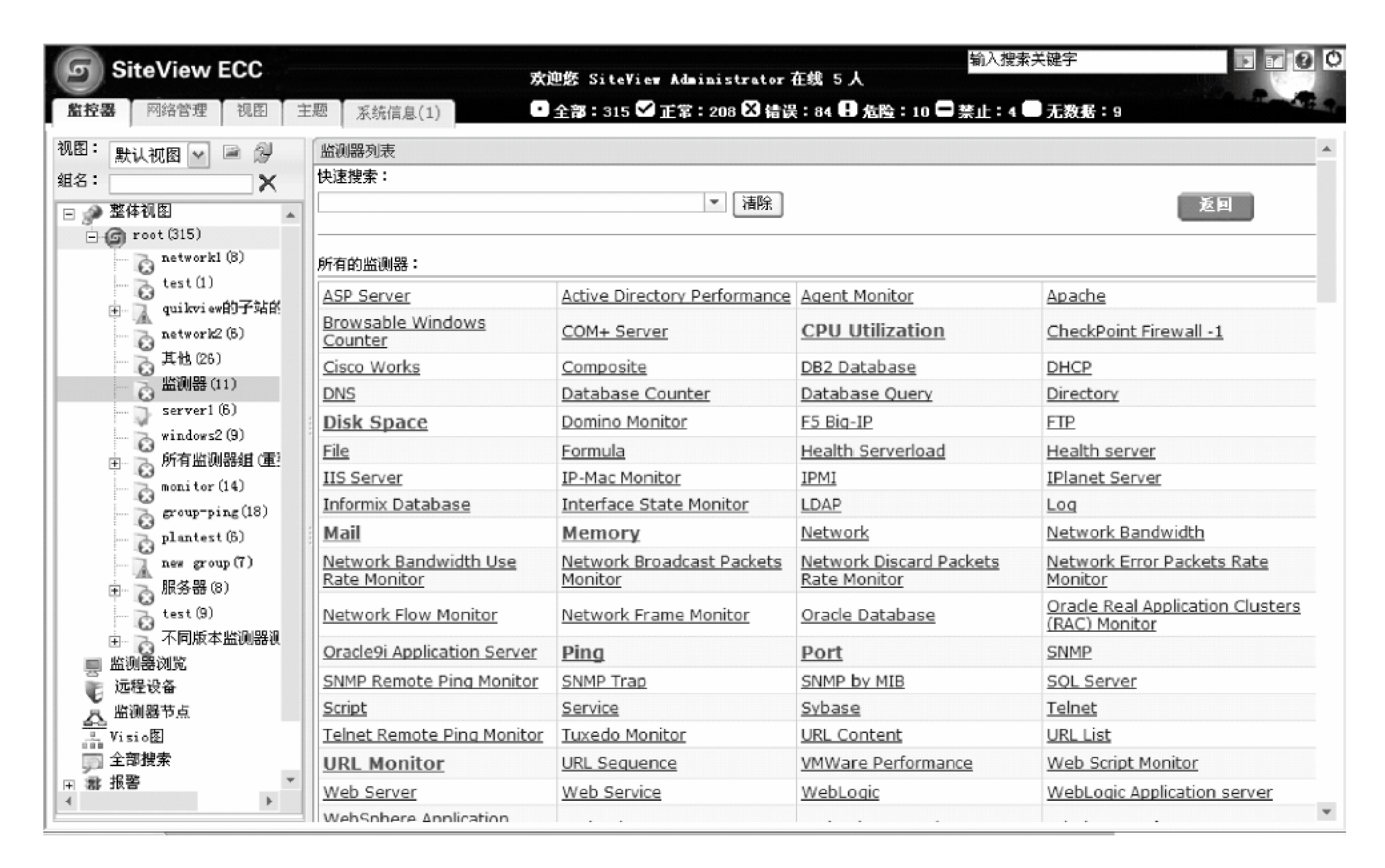


图 8-25　监测器的列表

Service、CpuDetailRate、FilterEventLog、Process、Physical Memory、SysLog 和 SSL。单击要添加的监测器菜单，进入添加监测器窗口，输入完毕后单击“添加”按钮即可实现监测器的添加。

如果已经在设备里添加了监测器，并且监测器的数据都正常，那么树形结构中该设备名称前的图标和监测器列表中的状态按钮均显示为绿色。可以看到，在名称、编辑、刷新的位置都有链接，单击后可以看到它的相关信息。

监测器提供了详细信息的视图，分为图表、数据、趋势报表、鱼眼视图 4 个选项卡，可以形象地记录当前监测器某月、某周、某日或者某时段的运行情况。

（2）浏览监测器

监测器浏览可根据不同类型的过滤条件快速查看服务器内各种状态的监视器信息，方便用户按不同需求进行查询、统计、汇总。同时，在查询结果中，可以通过鼠标单击列表中的各个链接导航到查看设备和监测器的详细信息窗口、编辑当前监测器窗口，并实现即时刷新当前监测器、获取最新的监测器数据等功能。

单击控制台树的“监测器浏览”打开监测器浏览的主界面。系统预设了 2 个筛选条件，可查看浏览次数最多的监测器和最新添加的监测器，这些预设条件不能修改和删除。同时，系统将添加的筛选条件保存在客户端，当连接其他的服务器时，这些筛选条件同样能派上用场，系统将根据它们调出当前服务器中符合条件的数据，如图 8-26 所示。

（3）设置监测器

监测器设置用于批量修改和设置监测器的监测频率、报警条件。在整体视图中，可以对单个监测器进行编辑，修改它的监测频率和报警条件；但若想将所有 Windows 服务器下的 CPU 监测器的监测频率进行修改，一个一个地编辑会非常麻烦和浪费时间；通过监测器设置，可以一次性完成 CPU 监测器的监测频率修改。



图 8-26　监测器浏览页面

① 修改监测频率

单击控制台树的"监测器设置",打开监测器设置的主界面。以修改 Windows 服务器的 CPU 监测器为例,在监测器树中选择需要修改的监测器,系统自动将其加载到监测器显示框中,如图 8-27 所示。



图 8-27　"监测器设置"页面

选好了要修改的监测器后，在“基础信息”选项卡中输入监测器频率，即完成了批量修改监测频率。如果要继续修改报警条件，单击“应用”按钮，然后选择监测器，修改报警条件，反之，单击“确定”按钮。系统会将这一批修改的数据显示在监测器设置主界面的结果窗口中。

② 修改报警条件

同修改监测频率的操作方法类似，打开批量修改监测器的窗口后，勾选需要修改的监测器，在修改设置中选择“报警条件”。

在监测器类型下拉列表框中，系统将选中的监测器进行了分类，选中其中一种类型，进入编辑警告条件窗口，设置方法同增加监测器，全部输入完成后，单击“确定”按钮即可实现批量修改报警条件。

③ 错误校验

当监测器发生错误时，根据设定的错误校验时间，系统将再一次去服务端获取数据。初始设置在添加监测器窗口的“高级选项”选项卡中设定，操作过程与修改监测器频率和报警条件相同。

4）拓扑图

通过 Microsoft Visio 可以发布拓扑图，当然在使用 Visio 拓扑图功能之前，必须先安装 Visio 2003 和 SiteView ECC 提供的 Visio 拓扑图发布插件。

插件通过“拓扑视图”下载原拓扑图发布安装程序来实现插件的安装。下载新拓扑图发布插件，并复制插件 Siteview. vsl 到 Microsoft Office\Visio11\2052\Siteview\目录。

Visio 拓扑图不仅可以使用 SiteView ECC 提供的模板来绘制拓扑图，还可以在用户原有的拓扑图上稍加改动，就可以使用 SiteView ECC 提供的 Visio 拓扑图功能了。具体操作如下：

（1）启动 Visio，打开原有的拓扑图文件。

（2）选择任一个图形（节点），右击，并从快捷菜单中选择“形状”→“自定义属性”命令，弹出“自定义属性”对话框。

（3）单击“定义”按钮，弹出“自定义属性”对话框。

（4）删除系统所有默认的自定义属性，单击“新建”按钮，在“标签”文本框内输入“实体 IP”，在“名称”文本框内输入“SV_IP”，在 Value 文本框内输入 IP 地址。

（5）单击 OK 按钮，回到“自定义属性”对话框。

（6）单击 OK 按钮，回到所打开的文档。

（7）使用 SiteView ECC Publish 发布拓扑图，单击“工具”→“加载项”→“SiteView Publish”进行发布。

SiteView Publish 要求提供 SiteView 的服务器地址和端口号，SiteView 系统默认的端口是 6688，在“SiteView 的地址”文本框内输入正确的地址，单击“确定”按钮后拓扑图就会发布到指定的机器上。拓扑图发布成功后，会在拓扑视图的拓扑列表中显示。每个拓扑图发布后，提供了编辑、删除、下载拓扑图的功能，用户可以根据需要进行操作。如图 8-28 所示为 Visio 管理窗口。

每个拓扑图发布后，提供了编辑、删除、下载拓扑图的功能，用户可以根据需要进行操作。

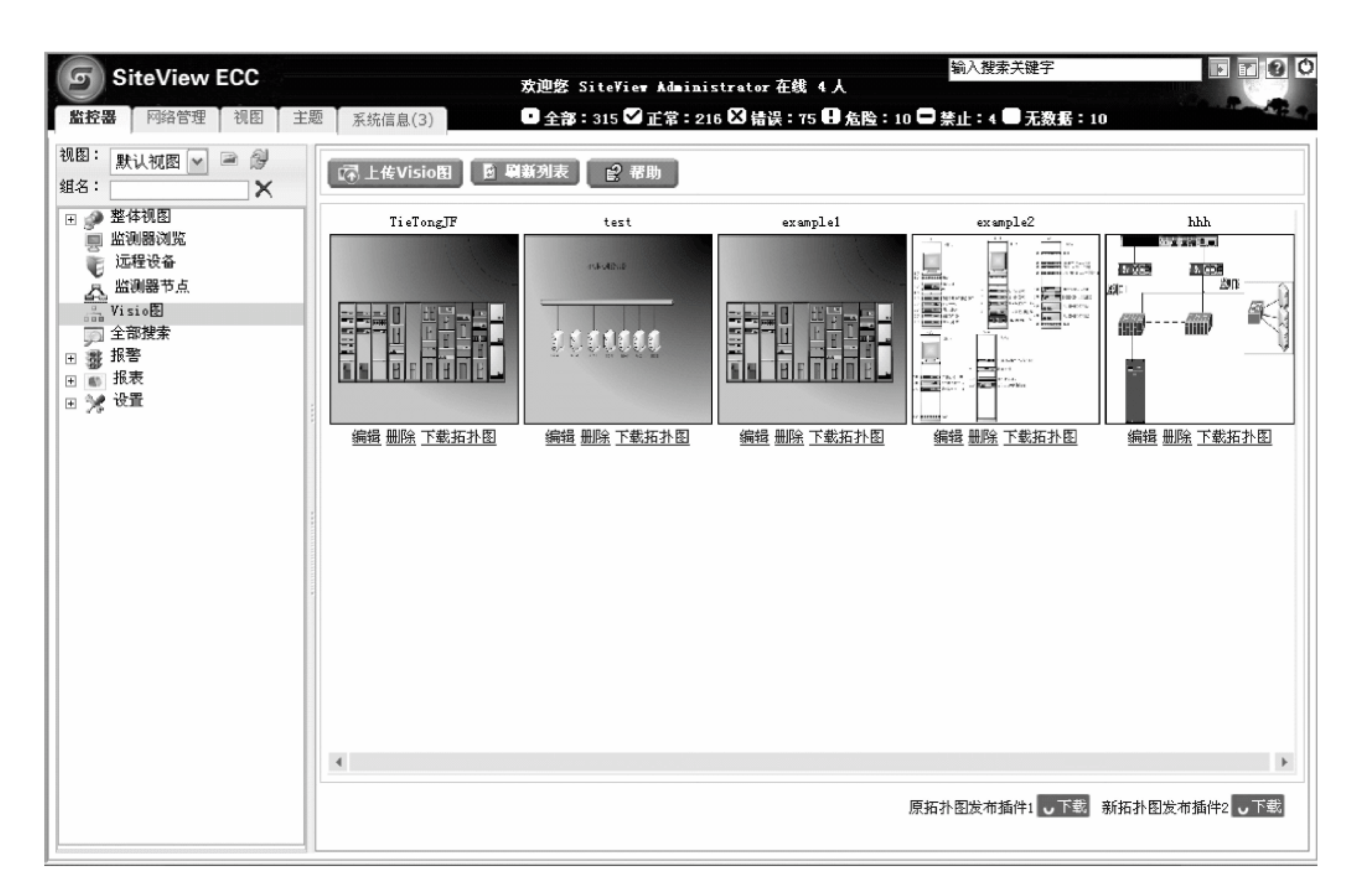


图 8-28 Visio 管理窗口

5）报警

SiteView ECC 提供了完善的报警功能。当某个监测器的状态超过事先设定的阈值时，系统将自动做出相应响应，包括电子邮件、手机短信、脚本、声音等报警提示。

报警模块包括报警规则和报警日志两大功能。报警规则包括添加、删除、禁止、允许、刷新、编辑报警等功能。报警规则的添加报警操作如下：

(1) 在 SiteView ECC 左侧功能导航栏选择“报警”→“报警规则”，然后在显示的页面中单击“添加”按钮进入报警选择页面，报警规则具体包括 E-mail 报警、短信报警、脚本报警和声音报警。用户可以根据自己的情况选择具体的报警类型，下面以 E-mail 报警为例进行设置。

(2) 单击“报警规则”，在“报警选择”页面中单击“E-mail 报警”，进入具体添加 E-mail 报警页面，添加报警规则的页面也是由两个部分组成，左侧是报警所监测的对象，在这些设备和监测器旁都有复选框，在右侧需要输入具体的页面描述。图 8-29 是选择用短信报警的设置。

6）报表管理

SiteView ECC 8.1 默认有统计报告、趋势报告、TopN 报告、对比报告、时段对比报告、监测器信息、SysLog 查询等七大类报告，增强了对数据的挖掘、计算、统计和分析。用户可以根据需要，自定义报告的内容和表现形式，系统会自动生成图表、图形、数据表等实时报告和历史报告。实时报告可以随时查看最近 40 次的监测数据；历史报告根据不同 IT 运维人员的要求，自动生成不同监测参数组合的任意时间段的性能分析报告，并可自动将报告定时发送到指定邮箱。



图 8-29　短信报警的设置对话框

报表模块可以提供实时的和基于天、周和月的不同报告，可指定时间生成不同监测参数组合的报告，供用户分析诊断系统状况。预测一段时间内的趋势情况，及不同监测器的对比与不同时间同一监测器的对比等，可进行相关的统计分析；提供多种灵活的查询条件，生成各式报表输出，并提供了直观简明的线状图、曲线图等不同的图形，还可导出成 Excel 表格、图片等文件格式，方便打印和保存。下面以趋势报告为例进行说明。

趋势报表表明一段时间内的趋势情况。报表通过八种类型的图形表现选定的数据在一段时间内的运行情况，因此可以根据之前监测的运行情况统计分析，得出每个参数的运行情况值，通过提供的预测值，可提早监控容易出问题的参数，提早对系统进行升级维护，从而防止意外的服务停顿事件。

通过统计监测器的正常运行时间、危险、错误、最新值和阈值，对监测器一个时间段内的最大值、最小值和平均值，及最近一次数据和最大值时间进行统计，并提供不同时间的数据变化图，来方便用户对该监测器以后的运行情况进行预测。用户并可以根据需要选择不用的监测时间段，从几个小时到几个月不等。

通过查看趋势报告，用户可以查看当前监测器的信息和报告图，打开趋势报告，如图 8-30 所示。



图 8-30　趋势报告页面

8.3.2　IBM Tivoli 管理系统

1. 企业 IT 系统管理

IT 系统管理已经有二十几年的历史，其发展历程已经从无序、混沌的运维管理，经过简单的对重要资源运行的自动监视，发展至今天的企业级 IT 系统管理。

如图 8-31 所示，IT 系统管理可以看成由服务支持和服务提供两部分工作组成。服务支持是 IT 管理者每天进行的日常管理工作，工作重点偏重于 IT 技术；服务提供是将管理数据转化为决策信息，工作重点偏重于从业务视角来看待问题。

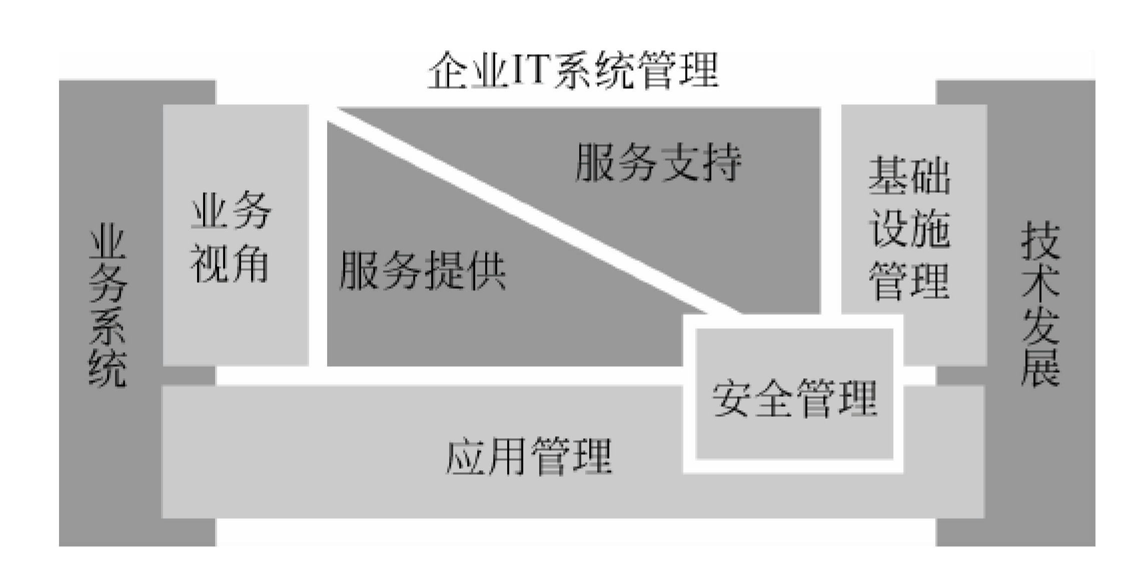


图 8-31　企业 IT 系统管理的构成

随着企业规模的不断扩大，业务应用的持续增加，其 IT 基础设施的架构越来越复杂，单纯凭某个工具或某个人，已经不能胜任如此大的工作量和满足业务紧迫性的要求，必须有一整套的企业 IT 系统管理的解决方案。

2. IBM Tivoli 系统管理结构

IBM Tivoli 的管理结构分为系统及应用监控、事件关联和自动化和业务影响管理三层。为了满足复杂 IT 资源管理需要，IBM Tivoli 将可靠性管理分成实时监控和历史数据分析

两个方面，每个方面又分成不同的几个层次，如图 8-32 所示。

实时监控

业务影响管理
- 将IT管理与业务目标链接
- 保证客户服务水平
- 通过预测性计划，改善投资效率
- 将数据转化为信息

时间相关及自动化
- 了解交叉域的相互作用
- 通过快速解决问题提高可用性
- 清除潜在的失败点

系统和应用监控
- 目标前瞻式识别，通知问题
- 自动发现关键资源
- 自动问题修复
- 相应时间分析

历史数据分析

服务水平管理
- 主动判断故障事件对业务的影响
- 查看物理环境上的业务流程情况
- 确认最终用户的服务等级
- 分析历史数据，预报将来的服务水平

统计报表和预测分析
- 提供备管理对象的历史数据
- 统计报表和Web输出
- 自动统计、分析

图 8-32　Tivoli 管理系统的层次

不同的客户可能需要不同的管理层次，对于相对规模较小的客户而言，可以仅仅利用实时监控来完成对系统资源的自动管理；对于系统相对复杂的客户，需要将多种 IT 资源纳入到一个管理分析中，此时事件关联和分析就是非常重要的；对于大型业务处理系统的客户，需要由 IT 系统来维持其业务的运作和发展，对于 IT 系统的考核已不能简单地通过宕机时间来判断，需要通过对业务系统影响的情况来判断每次故障的大小和破坏程度，这就是业务影响管理。

IT 管理的另一个目标就是实现量化管理，通过管理数据来分析系统的状况、变化趋势、将来可能遇到的问题等。企业管理决策层更需要确切的数据来分析系统容量情况、性能情况，从而为其决策提供有用的依据。Tivoli 提供了集中的统计报表系统、预测分析系统和服务水平管理系统，这些事后分析都是基于 Tivoli 的管理数据来说明整个系统的过去、现在和将来的状况。

如图 8-33 所示，IBM Tivoli 软件通过如下的三层管理模型实现了面向业务影响管理的目标。在每一管理层，IBM Tivoli 软件都有特定的管理目标，从底层的单独系统资源的管理，到中间层的多资源事件的关联及自动化，直至最上一层的业务影响管理。

3. IBM Tivoli 系统管理解决方案

IBM Tivoli 系统管理软件可以满足各种类型企业在系统管理方面的需求，其中典型的解决方案包括网络管理解决方案、企业系统监控管理解决方案、企业业务影响管理解决方案、Web 管理解决方案和企业资产管理解决方案等。

1）网络管理解决方案

IBM Tivoli 网络管理解决方案，以 IBM Tivoli NetView 作为网络管理平台；同时配合 IBM Tivoli Switch Analyzer，可以对网络第二层实施监控；所有网络监控的事件，可以无缝地发送到 IBM Tivoli Enterprise Console，与其他系统管理监控事件进行关联；同时，所有网络性能数据可以通过 Tivoli Data Warehouse 进行存储，以便生成网络管理性能报告。Tivoli NetView 控制台如图 8-34 所示。

IBM Tivoli系统管理层次	IBM Tivoli系统管理目标
业务影响管理 •将IT管理与业务目标链接 •抱枕客户服务水平 •通过预测性计划，改善投资效率 •将数据转化为信息	•提取操作数据和经验 •改善未来的性能 •创建服务水平协定(SLA) •衡量SLA承诺方面的交付情况
事件相关及自动化 •了解交叉域的相互作用 •通过快速解决问题提高可用性 •清除潜在的失败点	跨复杂范围的资源和的自动化关联 •主机系统 •分布式客户机/服务器环境 •基于Web的环境 •中间件、网络、操作系统和硬件
系统和应用监控及配置操作管理 •目标前瞻式识别，通知问题 •自动发现关键资源 •自动问题修复 •响应时间分析 •自动化软件分发、清单和许可证管理 •自动在主机和分布式系统间调度作业	•前瞻式监视资源 •识别问题，确定其根本原因，通知其它系统挂起问题，自动采取动作修复问题并防止同样问题再次发生 •中央控制点向多个地点快速高效率部署 •提供全面的软硬件资产目录降低成本 •延伸集中式作业调度管理的范围

图 8-33　Tivoli 管理系统的层次与目标



图 8-34　Tivoli NetView 控制台

通过 IBM Tivoli 网络管理解决方案，可以实现的功能主要包括以下几个方面。

(1) 网络拓扑管理

Tivoli NetView 能够自动发现联网的所有 IP 节点，包括路由器、交换机、服务器、PC 等，并自动生成拓扑连接。NetView 提供按照网络节点所在的地理位置对网络拓扑图进行客户化的功能，使之与实际的网络结构更加吻合。

(2) 网络故障管理

网络故障管理是网络管理的核心,网管软件应当能够及时发现网络的故障,按照故障的轻重缓急产生不同的报警,并且具备对故障事件自动处理的能力。Tivoli NetView 图形化的网络 IP 拓扑结构,使网络管理员可以迅速方便地发现区域网上出现故障的 IP 资源并帮助管理员分析故障原因。当网络中的设备出现故障、机器死机或网络链路中断时,NetView 会及时在屏幕上显示报警信号,并在拓扑图中将该设备置成红色,便于网络管理人员发现诊断。

(3) 网络性能管理

网管人员需要了解网络实时的性能状况,需要能够对网络性能作出分析和预测,并生成相应的报表。Tivoli NetView 的 SnmpCollect 功能,能够自动采集重要的网络性能数据,如 IP 流量、带宽利用率、出错包数量、丢弃包数量、SNMP 流量等,并设置相应的阈值,当所采集的数据达到阈值时,能够触发报警或者定义好的自动操作。可以用图形的方式显示这些网络性能数据的变化情况,也可以将这些数据存放于关系型数据库系统中,以便于检索和分析。

Tivoli Data Warehouse 将为网络性能管理提供集中的历史统计和报表分析,能够帮助管理人员从大量数据中及时发掘出可以用作判断网络运行状况的数据,能够生成各种报表和图形化的分析报告。

(4) 网络设备管理

Tivoli NetView 支持业界标准的 API,能够与主要网络设备厂商的设备管理软件,如 CiscoWorks、Nortel(Bay) Optivity、3com Transcend 等方便地进行集成,从而能够统一从 NetView 的 Console 对各种网络设备进行监控和配置。

通过使用 Tivoli NetView 与网络设备管理软件的集成,管理人员可以全面地管理网络、网络设备、网络性能,及时获取网络故障的信息,从而在最短时间内解决网络故障。

(5) 管理权限分配

Tivoli NetView 可以为管理员定义不同的管理角色,不同的管理员可以被授权管理不同地址范围的设备,而且没有权限管理的设备不会在拓扑图中显示出来。

(6) Web 管理功能

Tivoli NetView 通过 Web Console 实现分布式管理界面。NetView Web Console 为用户提供了一个灵活、可配置的环境,以便用户可以访问网络状态和配置信息。

使用 Web Console 可以浏览交换机的端口状态、路由器状态、MAC 地址状态等,方便了交换机管理。

(7) 支持 MPLS 管理功能

NetView 7.1 支持对 MPLS 设备的识别,并能对有关 MPLS 的数据进行查询。NetView 可以管理 LSR(Label Switch Routers)设备。

(8) 交换机的故障定位

IBM Tivoli Switch Analyzer 提供第二层交换设备发现功能,识别包括第二层和第三层交换设备在内的设备之间的关系。正确的关联分析,无论其根源是一个 IP 寻址的端口还是一个第二层的局域网交换机上非 IP 寻址的端口、板卡或插件。另外,IBM Tivoli Switch Analyzer 还扩展了 IBM Tivoli NetView 和 IBM Tivoli Enterprise Console 的故障根源分析

功能。

2）企业系统监控管理解决方案

IBM Tivoli 软件通过集成的企业系统监控管理解决方案，帮助企业在广度和深度方面解决当前的 IT 系统监控管理所面临的挑战。IBM Tivoli 监控解决方案，通过提供跨越广泛的软件工具的统一界面，简化了管理人员所面对的复杂性。IBM Tivoli 企业系统管理解决方案体现在电子商务环境的如下两个不同的层面。

（1）系统和应用监控

IBM Tivoli 系统和应用监控解决方案，在每个独立资源的层次更容易地收集性能参数、分析问题的原因并在其影响其他资源之前自动修复许多问题。这是通过带有前瞻分析组件（Proactive Analysis Components）实现的。Tivoli 监控解决方案也被设计成支持其他 Tivoli 系统监控性能与可用性管理产品。

IBM Tivoli 系统和应用监控解决方案的核心产品是 IBM Tivoli Monitoring，这是个强劲的多用途监视引擎。其所采用的新技术，能够为所用环境中受到监视的绝大多数或全部资源部署单一监视解决方案。这种先进技术可以通过系统监视器分享共同的报告机制和图形用户界面，并且具有产生历史报表的共同数据中心库。

在此基础上，IBM Tivoli 系统和应用监控管理解决方案，能够监视多种执行类似任务的应用或资源，可以对以下资源实施监控：企业中 mySAP. com R/3、Sieble 等应用，IBM WebShpere MQ 等中间件，DB2、Informix、Oracle 等数据库，Domino、Web 服务器等。

（2）事件相关及自动化

当问题涉及多个资源时，IBM Tivoli 企业监控系统管理解决方案通过事件关联及自动化层次实现对问题的根源分析。

在系统和应用监控解决方案基础上，IBM Tivoli 事件关联及自动化解决方案提供了一个记录用户的 IT 系统和网络的整体健康状况的广泛的、全景窗口。它们可以自动地、智能地组合来自不同资源的信息，并关联特定的事件，帮助系统管理员跨多个系统、网络、应用和硬件来确定问题的根源。它们也可以使许多系统管理任务自动化，使企业能够前瞻式地解决问题并防止其再度发生。

IBM Tivoli 事件关联及自动化解决方案具有很好的开放性，除了可以对系统和应用管理、配置和操作管理层传送来的事件进行关联外，还能够与第三方的应用和管理软件，甚至是客户自己的应用的事件进行集成。IBM Tivoli 事件关联及自动化的核心产品是 IBM Enterprise Console（企业控制台）。

通过这两层管理解决方案，IBM Tivoli 系统管理解决方案可以实现企业 IT 级的系统管理的几乎所有功能，保证系统、中间件、数据库和应用的监控运行，并能在出现问题时快速判断问题的根源，尽快解决问题。

3）企业业务影响管理解决方案

IBM Tivoli 的企业业务影响管理解决方案可以帮助企业将 IT 资源的性能与所服务的内部客户的业务需求相匹配，让管理人员以系统和网络如何支持一个特定业务流程或特殊业务线的方式来看待管理数据。通过实施这些解决方案，企业可以了解所需要的与客户或内部客户建立的有意义的 SLA，帮助预测或防止可能使 IT 管理不能达到服务水平目标的事件。

IBM Tivoli 企业业务影响管理解决方案由 IBM Tivoli Business Systems Manager（业务系统管理器）和 IBM Tivoli Service Level Advisor（服务水平顾问）两个核心产品构成。IBM Tivoli Business Systems Manager 提供的是单一的、完全集成的及可扩展的业务系统管理产品。同时，IBM Tivoli Service Level Advisor 可以提供服务水平管理的服务和相关报告。

总之，Tivoli 业务系统管理器和服务水平顾问结合在一起，能够保证用户跨整个管理基础设施，从可操作和可预测的角度来管理用户的服务水平。

4）Web 管理解决方案

IBM Tivoli Web 管理解决方案提供了一套综合的方法以确保企业的网站提供最佳性能和可靠性。企业可以安全地管理 Web 基础设施、给用户期望的服务，同时保持竞争优势。IBM Tivoli Web 管理解决方案包括 IBM Tivoli Monitoring for Web Infrastruture、IBM Tivoli Monitoring for Transaction Performance 和 IBM Tivoli Web Site Analyzer 三个模块。

（1）IBM Tivoli Monitoring for Web Infrastructure 是一个优化应用服务器和其所连接的 Web 服务器的性能和可用性的关键工具。它提供了一个单一控制点，可以让 IT 管理人员了解 Web 环境中关键元素的健康状况。它也可以使管理人员快速识别问题，在需要时向相关人员报警，并提供自动解决问题的方法。Tivoli Monitoring for Web Infrastructure 还提供了一个实时性能健康状况视图，并可以将数据传送到共享数据仓库，形成历史报告及分析。这个软件提高了 IT 管理人员的工作效率，保证了对重要 Web 基础设施的性能和可用性的优化。

（2）IBM Tivoli Monitoring for Transaction Performance 可以帮助用户测量实际客户响应时间、定期执行预录制交易和扫描网站来发现潜在问题，有助于维持电子商务和交易的可用性和性能。IBM Tivoli Monitoring for Transaction Performance 借助于其独具一格的交易性能管理方式，帮助衡量和主动改善网站访问者和客户的体验质量。它使用先进的技术跟踪用户交易，将总计响应时间分解成各组件部分，并且允许看到该交易在基础架构内的路径。基于 Web 的实时界面，可查看客户正在感受到的响应时间，而历史报告则可帮助简化长期趋势分析。

（3）IBM Tivoli Web Site Analyzer 是一个企业级 Web 分析工具，它将分散的 Web 数据转化为有价值的电子商务业务智能。它提供了一个清晰的图画，显示用来支持业务成果管理的电子商务基础架构的整体健康状况和集成性。

通过捕获、分析、存储和报告 Web 站点的使用率、健康状况、集成性和站点内容，IBM Tivoli Web Site Analyzer 可以显示访问者与网站的交互性和网站的整体性能。可以利用这种分析的结果来优化网站，从而提高客户忠诚度和电子商务的效能。Web Site Analyzer 可以为特定的意图或商务活动跟踪指定的访问者或客户群所访问的页面内容和购买的产品，也可以指出在哪方面减少投资或可能的 Web 浏览变更，以便减少所访问的 Web 页面或产品页面。

同时，IBM Tivoli Web Site Analyzer 可以帮助用户确定是将广告投资通过在线方式还是其他方式进行，例如基于产生的流量和实际的利润，确定与哪一家电子商务合作伙伴进行合作。它通过多种方式收集数据的模型，将所有分布式的 Web 服务器的日志文件集成到一

个单一开放的数据仓库。另外，它提供了一个更实时的方法，通过 IBM Tivoli Web Site Analyzer Web Tracker 功能动态捕获 Web 页面信息。通过采用所有这些技术，IBM Tivoli Web Site Analyzer 可以简化 Web 服务器活动的报告、Web 访问者的统计分析和客户行为。

由 IBM Tivoli Web Site Analyzer 生成的信息可以更深入地了解用户的 Web 体验和电子商务的性能，从而可以对所管理的电子商务基础设施做出更准确的趋势评估和前瞻性的决定。通过将 Web 使用率和流量信息与性能和可用性矩阵相关联，可以帮助优化企业与客户、企业与企业及企业与雇员之间 Web 站点的有效性。它的卓越性能和全面的分析，可以帮助 IT、市场和销售人员进行决策。

5）企业资产管理解决方案

IBM Tivoli 企业资产管理解决方案，能够帮助企业控制动态电子商务环境中的复杂性，最大限度地提高技术投资回报率，提供安全且高度可用的电子商务基础架构。IBM Tivoli 资产解决方案不仅有助于满足当今维持强劲且高效率电子商务基础构架的需求，而且能够提供未来扩展和新技术的基础。

IBM Tivoli 企业资产管理解决方案组合包括 4 个核心产品：IBM Tivoli Configuration Manager（配置管理软件）、IBM Tivoli License Manager（软件许可证管理）、IBM Tivoli Remote Control（远程控制）和 IBM Tivoli Workload Schedule（作业调度）。这 4 个软件能够单独使用，但也经常合在一起以帮助最大化集成的价值。跨数目巨大的端点进行扩展和对异构操作系统平台进行管理，均属于这些产品的内置功能。

（1）IBM Tivoli Configuration Manager 包含了软件分发和资产清单的功能。软件分发组件能够由中央控制点对多个系统和用户快速高效率地部署复杂的关键业务应用程序。Tivoli Configuration Manager 的资产清单组件，通过利用全面的软硬件资源目录（超过两万个千字且按季度更新），可高效率地规划和实施技术变更，因而能够帮助用户降低信息技术开支。

（2）IBM Tivoli License Manager 是一个高效的管理软件许可证的工具。通过先进的库存和报告能力，可以帮助业务部门准确得知需要什么软件许可证以及谁需要哪些许可证。通过使用 IBM Tivoli License Manager 可以极大地节省成本，只对需要的许可证付费；同时可以有效防范许可证的非法使用情况的发生；而且可以对未来软件的许可证数量进行预测。

（3）IBM Tivoli Remote Control 通过提供对桌面机和服务器的远程管理能力，以帮助实现电话解决问题的高比例和减少派遣信息技术人员的需要，从而降低信息技术支持的总成本。IBM Tivoli Remote Control 与 IBM Tivoli Configuration Manager 配合使用，可提供管理电子商务基础架构之变更和配置的强劲集成解决方案。

（4）IBM Tivoli Workload Scheduler 通过跨主机环境和分布式环境提供集成的调度能力，简化了系统管理员的任务。此解决方案具有智能日历和全面的操作员控制台；性能增强项目包括更高效率的任务执行自动化和通过速度的总体改善。

被称为容错代理（Fault Tolerant Agent）的新轻量级调度代理推动了扩展能力和性能的加强。其他新特性包括改善的数据管理和经由 XML 支持与基于 Web 报告能力的报告、跨工作负载的先进资源分享、改善的验证和加密特性。

8.4 本章小结

本章介绍了网络管理系统的基本概念和常用的网络管理工具。首先介绍了网络管理系统，包括网络管理系统的概念、分类、组成和结构等理论知识；然后介绍了网络管理常用的工具，包括服务器监控、网络性能监控、网络流量监控等工具；最后介绍了国内外有名的企业级的网络管理工具，如 SiteView ECC、IBM Tivoli 等。

本章需要重点掌握网络管理系统的逻辑结构，各功能模块间的关系，并掌握常用网络管理工具的使用方法。

习　题　8

一、选择题

1. 网络管理系统按作用可以分为三个部分，它们分别是(　　)。

A. 操作　　B. 管理　　C. 维护　　D. 运行

2. 从管理信息的组织和管理角度考虑，MIB 的功能一般包括(　　)三部分。

A. 支持服务　　B. 检索服务　　C. 构造服务　　D. 访问服务

3. 故障管理需要从(　　)得到当前的运行分析结果，从配置数据库得到设备配置信息。利用上述信息和网络的事故报告，一旦确认发生故障，通过配置管理来修改配置参数，启动恢复行动，修复、替换或隔离故障部件。

A. 故障管理　　B. 计费管理　　C. 安全管理　　D. 性能管理

4. 性能管理需要从(　　)得到用户使用网络的详细记录，利用收集的统计数据和故障管理检测的故障情况，计算网络性能参数，一旦出现危险状态则向故障管理示警。

A. 故障管理　　B. 计费管理　　C. 安全管理　　D. 配置管理

5. 服务器监控工具所要监控的内容很多，总体可以分为监控服务器(　　)三大块。

A. 运行状态　　B. 通信量　　C. 使用结果　　D. 拓扑结构

6. 网络性能决定着网络服务的质量，网络性能不仅与交换机和路由器等设备的性能相关，而且与(　　)也有很大关系。

A. 线路长度　　B. 线路种类　　C. 线路质量　　D. 线路结构

二、简答题

1. 什么是网络管理系统？
2. 简述网络管理系统的逻辑组成。
3. 简述网络管理系统的结构。
4. 网络管理系统各功能间的关系是什么？
5. 网络性能的指标有哪些？
6. 我国网络管理系统的产品有哪些？

第9章　网络故障诊断与维护

无论规划设计得多么周密，施工多么严谨，设备多么先进，网络问题的出现是不可避免的，所以无论什么样的网络都必然会面临着大量的故障诊断、恢复与维护工作。出问题并不可怕，关键是如何迅速恢复网络的功能，保证业务的开展。本章将介绍网络故障诊断与维护的相关知识。

9.1　网络故障诊断概述

计算机网络是一个复杂的综合系统，其故障的诊断是一门综合性的技术，涉及网络技术的诸多方面。网络故障诊断以网络原理、网络配置和网络运行知识为基础。从故障现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源，排除故障，恢复网络正常运行。保障和维护网络正常、稳定、安全地运行，提高网络应用的效率是网络管理的重要目标。

1. 网络故障诊断的目的

（1）确定网络的故障点，恢复网络的正常运行。

（2）发现网络规划和配置中的瑕疵，改善和优化网络的性能。

（3）观察网络的运行状况，及时预测网络通信质量。

2. 网络故障产生的原因

产生网络故障的原因很多，可能是硬件设备的原因，如网卡、交换机、服务器等；也可能是来自软件的设置错误或其他错误引发的各种问题，如协议配置、驱动程序配置、负载不均衡产生的“瓶颈”等问题。但从 OSI 通信模型来看，网络的故障产生可能来自以下几方面：

（1）物理层问题，由于物理设备相互连接失败或者硬件及线路本身引起的问题。

（2）数据链路层问题，包括网络设备接口的配置等问题。

（3）网络层问题，由于网络协议配置或操作引起的错误。

（4）传输层问题，由于性能或通信拥塞引起超时等问题。

（5）应用层问题，包括操作系统、网络应用程序自身中的软件错误。

从 OSI 数据通信模型的原理可知，诊断网络故障应该是一个从最底层开始逐层向上进行的过程，即首先检查物理层，然后检查数据链路层，以此类推，只有这样才能够有效地查清出现网络故障的原因所在。

3. 网络故障排除的方法

OSI 的层次结构为管理员分析和排查故障提供了非常好的组织方式。由于各层相对独立，按层排查能够有效地发现和隔离故障，因而一般使用逐层分析和排查的方法。

通常有两种逐层排查的方式，一种是从低层开始排查，适用于物理网络不够成熟稳定的情况，如组建新的网络、重新调整网络线缆、增加新的网络设备；另一种是从高层开始排查，适用于物理网络相对成熟稳定的情况，如硬件设备没有变动。无论哪种方式，最终都能达到目标，只是解决问题的效率有所差别而已。

具体采用哪种方式，可根据具体情况来选择。例如，遇到某客户端不能访问 Web 服务的情况，如果管理员首先去检查网络的连接线缆，就显得太悲观了，除非明确知道网络线路有所变动。比较好的选择是直接从应用层着手，可以这样来排查：首先检查客户端 Web 浏览器是否正确配置，可尝试使用浏览器访问另一个 Web 服务器；如果 Web 浏览器没有问题，可在 Web 服务器上测试 Web 服务器是否正常运行；如果 Web 服务器没有问题，再测试网络的连通性。即使是 Web 服务器问题，从底层开始逐层排查也能最终解决问题，只是花费的时间太多了。如果碰巧是线路问题，从高层开始逐层排查也要浪费时间。

在实际应用中往往采用折衷的方式，凡是涉及网络通信的应用出了问题，直接从位于中间的网络层开始排查，首先测试网络连通性，如果网络不能连通，再从物理层（测试线路）开始排查；如果网络能够连通，再从应用层（测试应用程序本身）开始排查。

4. 一般网络故障排除的步骤

（1）确定故障的具体现象，分析造成这种故障现象原因的类型。例如，主机不响应客户请求服务，可能的故障原因是主机配置问题、网络接口卡故障或路由器配置命令丢失等。然后根据故障的性质和影响范围进行故障定位。

（2）收集需要的用于帮助隔离可能故障原因的信息。从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。

（3）根据收集到的情况考虑可能的故障原因，排除某些故障原因。例如，根据某些资料可以排除硬件故障，把注意力放在软件原因上。

（4）根据最后的可能故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样可以容易恢复到故障的原始状态。如果一次同时考虑多个故障原因，试图返回故障原始状态就困难多了。

（5）执行诊断计划，认真做好每一步测试和观察，每改变一个参数都要确认其结果。分析结果确定问题是否解决，如果没有解决，则继续测试观察，直到故障现象消失。

（6）记录解决方案，确定预防措施。在问题解决以后，作为合格的管理员，还需要将问题解决过程中的相关记录整合成文献，以备后用。同时，还要制定同样问题再次产生的预防措施，以主动的方式进行网络管理活动。

9.2　网络故障的分类

在现行的网络管理体系中，由于网络故障的多样性和复杂性，网络故障分类方法也不尽相同。根据网络故障的性质可以分为物理故障与逻辑故障；也可以根据网络故障的对象分为线路故障、路由器故障和主机故障等。

1. 按网络故障的性质分类

（1）物理故障

物理故障是指设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。比如说，网

络中某条线路突然中断，如已安装网络监控软件就能够从监控界面上发现该线路流量突然掉下来或系统弹出报警界面，更直接的反映就是处于该线路端口上的基于网络的管理信息系统无法使用。

另一种常见的物理故障就是网络插头误接，这种情况经常是在没有搞清网络插头规范或没有弄清网络拓扑结构的情况下导致的。

（2）逻辑故障

逻辑故障中的一种常见情况就是配置错误，就是指因为网络设备的配置原因而导致的网络异常或故障。配置错误可能是路由器端口参数设置有误，或路由配置错误导致路由循环或找不到远端地址，或者是网络掩码设置错误等。比如，同样是网络中某条线路故障，发现该线路没有流量，但又可以 ping 通线路两端的端口，这时很可能就是路由配置错误导致路由循环了。

逻辑故障中另一类故障就是一些重要进程或端口关闭，以及系统的负载过高。比如，路由器的 SNMP 进程意外关闭或死掉，这时网络管理系统将不能从路由器中采集到任何数据，因此网络管理系统失去了对该路由器的控制。这时，也是线路中断，没有流量，但用 ping 发现线路近端的端口 ping 不通。

2. 按网络故障的对象分类

（1）线路故障

线路故障最常见的情况就是线路不通，诊断这种故障可用 ping 检查线路远端的路由器端口是否还能响应，或检测该线路上的流量是否还存在。一旦发现远端路由器端口不通，或该线路没有流量，则该线路可能出现了故障。这时有几种处理方法，首先是 ping 线路两端路由器端口，检查两端的端口是否关闭了。如果其中一端端口没有响应则可能是路由器端口故障。如果是近端端口关闭，则可检查端口插头是否松动，路由器端口是否处于 down 的状态；如果是远端端口关闭，则要通知线路对方进行检查。进行这些故障处理之后，线路往往就通畅了。

如果线路仍然不通，一种可能就是线路本身的问题，看是否线路中间被切断；另一种可能就是路由器配置出错，比如路由循环了，远端端口路由又指向了线路的近端，这样线路远端连接的网络用户就不通了，这种故障可以用 traceroute 来诊断。解决路由循环的方法是重新配置路由器端口的静态路由或动态路由。

（2）路由器故障

事实上，线路故障中很多情况都涉及路由器，因此也可以把一些线路故障归结为路由器故障。但线路涉及两端的路由器，因此在考虑线路故障时要涉及多个路由器。有些路由器故障仅仅涉及它本身，这些故障比较典型的就是路由器 CPU 温度过高、CPU 利用率过高和路由器内存余量太小。其中最危险的是路由器 CPU 温度过高，因为这可能导致路由器烧毁。而路由器 CPU 利用率过高和路由器内存余量太小都将直接影响到网络服务的质量，比如路由器上丢包率就会随内存余量的下降而上升。检测这种类型的故障，需要利用 MIB 变量浏览器这种工具，从路由器 MIB 变量中读出有关的数据，通常情况下网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。而解决这种故障，只有对路由器进行升级、扩内存等，或者重新规划网络的拓扑结构。

另一种路由器故障就是自身的配置错误。比如配置的协议类型不对，配置的端口不对

等。这种故障比较少见,一般出现在使用初期,配置好路由器后基本上就不会出现了。

(3) 主机故障

主机故障常见的现象就是主机的配置不当。比如,主机配置的 IP 地址与其他主机发生冲突,或 IP 地址根本就在子网范围内不存在,这将导致该主机不能连通。还有一些服务设置的故障。比如 E-mail 服务器设置不当导致不能收发 E-mail,或者域名服务器设置不当将导致不能解析域名。主机故障的另一种可能是主机安全故障,比如,主机没有控制其上的 finger、rpc、rlogin 等多余服务。而恶意攻击者可以通过这些多余进程的正常服务或 bug 攻击该主机,甚至得到该主机的超级用户权限等。

另外,还有一些主机的其他故障,比如不当共享本机硬盘等,将导致恶意攻击者非法利用该主机的资源。发现主机故障是一件困难的事情,特别是别人恶意的攻击。一般可以通过监视主机的流量或扫描主机端口和服务来防止可能的漏洞。当发现主机受到攻击之后,应立即分析可能的漏洞,并加以预防,同时通知网络管理人员注意。现在,防火墙的安装已经比较普遍,如果防火墙地址权限设置不当,也会造成网络的连接故障,只要在设置使用防火墙时加以注意,这种故障就能避免。

9.3 网络故障的分层检查

不同类型的网络(以太网、令牌环、FDDI、ATM)各自的故障也不相同,由于以太网的形式已经被业界广泛采用,这里只介绍以太网的故障类型并以 OSI 七层模型分别讲解。

9.3.1 物理层故障

物理层的功能是在物理信道上透明地传输位流,物理层设备的主要任务就是解决数据终端设备与数据通信设备之间的接口问题。物理层互连的设备是中继器和集线器,它们在物理层间实现透明的二进制比特复制,以补偿信号衰减,以此来延长网络的长度。

网络物理层的故障主要是指网络设备的连接性能故障,包括网卡、交换机、集线器、路由器等,其常见的物理故障如下。

(1) 电气性能故障:主要指网络设备的端口提供的电平不正常(过高、过低),电压极性不正常。

(2) 传输模式故障:网络设备的数据传输有半双工、全双工、自适应多种模式。在数据传输过程中,可能发生模式人为设置错误,相互不匹配;或两端不能自动地建立正确的传输协商机制等。

9.3.2 数据链路层故障

数据链路层的功能是在相邻两节点间无差错地传送数据帧,为网络层提供服务。数据链路层互连的设备是网桥,网桥在网络互连中起到数据接收、地址过滤与数据转发的作用,它用来实现多个网络系统之间的数据交换。用网桥实现数据链路层互连时,互联网络的数据链路层与物理层协议可以是相同的,也可以是不同的。

在 OSI 七层模型中的第二层数据链路层的数据传输是以帧的形式表示的。帧错误的类型如下:

(1) 碰撞帧：在集线器构建的网络中，最常见的错误就是碰撞。根据 CSMA/CD 机制，当两个站点同时发送信息时就会产生碰撞。碰撞发生后，站点原先发送的帧会被破坏而不完整，形成碎帧。碰撞按照发生的位置划分为以下几种：本地碰撞、远端碰撞、延迟碰撞、远端延迟碰撞。以太网的有关规范不但明确地指出碰撞是正常现象以及出现的原因，而且强调适当的碰撞不会对以太网带来负面影响。但是，过多的碰撞产生可能是由于网络中不良因素或错误造成的，过多的碰撞也会导致网络性能的大幅下降。

(2) 短帧：一个比有效的最短帧(在前同步信号之后少于 64 个字节)还小，但帧检测序列(FCS)是正常的帧。出现短帧最常见的原因是网卡故障、网卡驱动程序损坏或设置错误。

(3) 帧过长：一个比法定有效的最大长度(1518 字节)还长的帧，以太网规范中没有规定其帧的 FCS 是否正常。造成帧过长的常见原因是网卡故障、网卡驱动程序损坏或设置错误，连接电缆和接地问题。

(4) 长帧：一个比法定有效的最大长度(1518 字节)还长但 FCS 是正常的帧。其出现可能的原因是软件设置有误或网卡驱动程序损坏。

(5) 帧校验序列错误：一般帧首的信息准确，但接收端的累加校验与帧尾的 FCS 不相符合，此错误又称循环冗余校验(CRC)错误。单一站点过多的 FCS 错误表明网卡或软件程序有问题。如果 FCS 错误与多个站点相关则说明电缆链路系统有噪声。

(6) 字节位错误：一般帧的结尾不是以标准的 8 位字节结束，即数据帧比标准的 8 位二进制码组成的字节多(或少)几位，这主要是由于软件驱动程序错误或碰撞造成的。

9.3.3 网络层故障

网络层互连的设备是路由器。网络层互连主要是解决路由选择、拥塞控制、差错处理与分段技术等问题。如果网络层协议相同，则互连主要解决路由选择问题；如果网络层协议不同，则需要使用多协议路由器。用路由器实现网络互连时，允许网络互连的网络层级以下各层协议是不同的。

网络层提供建立、保持和释放网络层连接的手段，包括路由选择、流量控制、传输确认、中断、差错及故障恢复等。

排除网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由；然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障，包括 RIP 或者 IGRP 路由协议出现的故障。例如，对于 IGRP 路由选择信息，只在同一自治系统号的系统之间交换数据，查看路由器配置的自治系统号的匹配情况。

在网络的运行中，经常会遇到因设备设置导致的网络错误，通常这些故障的排除没有适当的工具是很难完成的。这些常见的网络问题归结成以下几类：

(1) 错误：指可以导致网络的设备不能正常运行的网络问题。例如，IP 地址冲突、子网掩码错误、IP 地址是子网地址、IP 地址是子网广播地址、关键设备没有响应、DHCP 服务器提供了正在使用的 IP 地址、丢失 DHCP 给出的地址。

(2) 警告：对网络的正常运行没有影响，但可能属于设备设置错误的网络问题。例如，默认路由器没有响应、IP 子网的唯一设备、IPX 网络唯一设备、网络中唯一使用 IPX 类型的设备、Proxy ARP 响应本地 IP。

9.3.4 传输层故障

传输层的主要功能有：提供建立、维护和拆除传输层连接；选择网络层提供的合适的服务；提供端到端的错误恢复和流量控制；向会话层提供独立于网络层的传送服务和可靠的透明数据传送。

传输层故障的检查主要包括以下两个方面：

(1) 差错检查，如数据包的重发等。

(2) 通信拥塞或上层协议在网络层协议上的捆绑方面。

9.3.5 应用层故障

应用层是 OSI 环境与本地系统的操作系统和应用系统直接接口的一个层次。在功能上，应用层为本地系统的应用进程访问 OSI 环境提供手段，也是唯一直接给应用进程提供各种应用服务的层次。根据分层原则，应用层向应用进程提供的服务是 OSI 的所有层直接或间接提供服务的总和。

应用层故障检查主要包括以下 3 个方面：

(1) 操作系统的系统资源的运行状况。

(2) 应用程序对系统资源的占用和调度。

(3) 管理方面的问题，如安全管理、用户管理等。

9.4 网络故障诊断工具

9.4.1 软件工具

1. IP 连接测试——ping

ping 命令是 TCP/IP 协议内置的一个测试工具，主要通过发送 ICMP 回响请求消息，来验证与另一台计算机的 IP 连接。对应的回响应答消息的接受情况将和往返过程的时间一起显示出来。ping 是用于检测网络连接性、可达性和域名解析的主要 TCP/IP 命令。

例如，网络运行正常情况下，在命令提示符窗口中输入如下命令：

```
ping www.sina.com.cm
```

按回车键执行，所有发送的包均被成功接收，丢包率为 0，如图 9-1 所示。

```
C:\>ping sina.com.cn

Pinging sina.com.cn [61.172.201.194] with 32 bytes of data:

Reply from 61.172.201.194: bytes=32 time=150ms TTL=243
Reply from 61.172.201.194: bytes=32 time=156ms TTL=243
Reply from 61.172.201.194: bytes=32 time=156ms TTL=243
Reply from 61.172.201.194: bytes=32 time=156ms TTL=243

Ping statistics for 61.172.201.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 150ms, Maximum = 156ms, Average = 154ms
```

图 9-1 正常时的 ping 命令测试结果

正常测试结果中会连续出现类似“Reply from 61.172.201.194：bytes ＝32 time ＝150ms TTL ＝243”的语句。其中，150ms 表示从发送数据到收到回应经历的时间，如果超出限定时间后仍未收到回应，则视为连接超时，自动继续发送下一个测试数据包，系统默认的超时时间为 4000ms(4s)；TTL＝243 表示对方主机的 TTL 值为 243，根据 TTL 值一般可以确定该计算机使用哪种操作系统，例如 Windows XP/2000 系统的主机 TTL 通常为 128，而 UNIX 系统的主机 TTL 一般为 255。

另外，还可以通过测试数据包的数目和数据包的大小来确定网络的丢包率，如果丢包率非常高，虽然网络是连通的，但是其稳定性会非常差。指定数据包的大小，则是为了测试网络是否能够提供一定的带宽。例如，在命令提示符窗口中输入如下命令：

```
ping 202.96.69.38 －n 5 －l 1000
```

按回车键执行，其中发送数据包的数量为 5，数据包大小为 1000 字节，从测试结果可以发现丢包率的大小。通常情况下，丢包率低于 20％时不会影响到正常网页浏览等应用。

2. 路由追踪——tracert

通过递增 TTL 字段的值将 ICMP 消息发送给目标可确定到达的路径。所显示的路径是源主机与目标主机间的路径、路由器的近侧路由器接口列表。近侧接口是离路径中发送主机最近的路由器接口。

例如，追踪到新浪网的路由，在命令提示符窗口中输入如下命令：

```
tracert sina.com.cn
```

按回车键执行，命令成功执行，可以看到从本机到新浪网之间所经过的所有路由，如图 9-2 所示。

```
C:\>tracert sina.com.cn

Tracing route to sina.com.cn [61.172.201.194]
over a maximum of 30 hops:

  1     9 ms    15 ms    15 ms  116.3.48.1
  2    15 ms    15 ms    15 ms  61.189.72.169
  3    15 ms    15 ms    15 ms  124.93.252.33
  4    15 ms    15 ms    15 ms  218.61.254.73
  5    15 ms    15 ms    31 ms  218.61.254.165
  6    30 ms    31 ms    31 ms  219.158.12.145
  7    30 ms    30 ms    30 ms  219.158.5.218
  8   156 ms   155 ms   155 ms  219.158.32.170
  9   171 ms   171 ms   171 ms  202.97.46.41
 10   156 ms   155 ms   155 ms  61.152.86.41
 11   156 ms   155 ms   155 ms  61.152.87.110
 12   155 ms   156 ms   155 ms  222.73.175.130
 13   155 ms   156 ms   156 ms  61.172.201.194

Trace complete.
```

图 9-2　追踪路由

3. 路径测试——pathping

pathping 主要用于提供在来源和目标之间的中间跃点处的网络滞后和网络信息丢失。pathping 将多个回响请求消息发送到来源和目标之间的各个路由器，然后根据各个路由器返回的数据包大小计算其结果。因为 pathping 显示任何特定路由器或链接的数据包的丢失程度，所以用户可据此确定引起网络问题的路由器或子网。pathping 通过识别路径上的

路由器来执行与 tracert 命令相同的功能。然后，该命令根据指定的时间间隔定期将 ping 发送到所有路由器，并根据每个路由器的返回数值生成统计结果。

如果要查看远程主机的路径信息，由于到远程主机往往要经过多重路由，因此通常需要指定禁止解析成域名，以加快查询速度。在命令提示符窗口中输入如下命令：

```
pathping sina.com.cn －n
```

按下回车键，执行成功，结果如图 9-3 所示。

```
C:\>pathping sina.com.cn -n

Tracing route to sina.com.cn [61.172.201.194]
over a maximum of 30 hops:
  0  116.3.59.180
  1  116.3.48.1
  2  61.189.72.169
  3  124.93.252.33
  4  218.61.254.73
  5  218.61.254.165
  6  219.158.12.145
  7  219.158.5.218
  8  219.158.32.170
  9  202.97.46.41
 10  61.152.86.41
 11  61.152.87.110
 12  222.73.175.130
 13  61.172.201.194

Computing statistics for 325 seconds...
```

图 9-3　测试到远程主机新浪网的路径信息

当运行 pathping 时，将首先显示路径信息。此路径与 tracert 命令所显示的路径相同。接着，将显示约 400s（该时间随着跃点数的变化而变化）的繁忙消息。在此期间，命令会从先前列出的所有路由器和及其链接之间收集信息，结束时将显示测试结果。

4. IP 路由表——route

route 命令主要用于手动配置路由表，如添加或者删除一条路由等，是网络管理工作中应用较多的工具。使用不带参数的 route 命令可以显示其帮助信息。例如，若显示当前路由表中的所有项目，则在命令提示符窗口中输入如下命令：

```
route print
```

按回车键，执行成功，结果如图 9-4 所示。由于当前计算机的所有网卡均配置了 IP 地址，因此所有的这些项目都是自动添加的。

如果要显示 IP 路由表中以 10 开始的路由项目，在命令提示符窗口中输入如下命令：

```
route print 10.*
```

在 route 命令中支持通配符，删除一系列路由时同样可以使用这种方法。

5. 网络诊断工具——netsh diagnostic

可以使用 netsh 网络诊断命令从命令行管理操作系统和网络服务参数，同时进行相关的疑难解答。netsh 诊断环境的命令提示符是 netsh diag＞。netsh diag 环境是 Windows Server 2003 家族的新增内容，因此这些命令将不能在 Windows 2000 Server 环境下运行。

例如，要显示本机所有的 IP 地址，在命令提示符窗口中依次输入 netsh 和 diag 命令进入 netsh diag＞环境中，然后输入 show ip 命令并执行，显示包括本地主机的 IP 地址和网卡名称，如图 9-5 所示。

```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 e0 6f 4f f9 40 ...... Realtek RTL8139/810x Family Fast Ethernet NIC -
数据包计划程序微型端口
0x40004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     116.3.59.180    116.3.59.180       1
          0.0.0.0          0.0.0.0      192.168.1.1   192.168.1.178       2
       116.3.48.1  255.255.255.255     116.3.59.180    116.3.59.180       1
     116.3.59.180  255.255.255.255        127.0.0.1       127.0.0.1      50
  116.255.255.255  255.255.255.255     116.3.59.180    116.3.59.180      50
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.178   192.168.1.178      20
    192.168.1.178  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.1.255  255.255.255.255    192.168.1.178   192.168.1.178      20
        224.0.0.0        240.0.0.0    192.168.1.178   192.168.1.178      20
        224.0.0.0        240.0.0.0     116.3.59.180    116.3.59.180       1
  255.255.255.255  255.255.255.255     116.3.59.180    116.3.59.180       1
  255.255.255.255  255.255.255.255    192.168.1.178   192.168.1.178       1
Default Gateway:      116.3.59.180
===========================================================================
```

图 9-4　当前所有路由项目

```
C:\>netsh
netsh>diag
netsh diag>show ip

IP 地址
    1. [00000001] Realtek RTL8139/810x Family Fast Ethernet NIC
       IPAddress = 192.168.1.178
    2. [00524291] WAN 微型端口 (IP)
       IPAddress = 116.3.59.180
```

图 9-5　显示本机的 IP 地址

6. 显示 IP 地址信息——ipconfig

ipconfig 命令用于显示所有当前的 TCP/IP 网络配置值，刷新 DHCP 和 DNS 设置。使用不带参数的 ipconfig 命令可以显示所有适配器的 IPv6 地址或 Pv4 地址、子网掩码和默认网关。

例如，要查看本地计算机的详细网络配置信息，在命令提示符窗口中输入 ipconfig /all 并执行，将显示包括所有适配器的 IP 地址、子网掩码和默认网关，还包括主机的相关配置信息，如主机名、DNS 服务器、节点类型、网络适配器的物理地址等，如图 9-6 所示。

有的时候，网站 DNS 域名没变，但是 IP 地址改变了，这时就需要重新查询 DNS 服务器，重新建立 DNS 缓存，否则将连接不到服务器。方法是在命令提示符窗口输入以下命令：

```
ipconfig /flushdns
```

此命令的作用等同于在 Windows 操作界面下，右击托盘区域的"本地连接"小图标，在打开的"本地连接状态"对话框中选择"支持"选项卡，然后单击"修复"选项。

如果由于 IP 的租约到期或者是手动设置了不正确的 IP 地址而导致计算机无法上网，这时只需让此计算机重新从 DHCP 服务器获取一个 IP 地址就行了。首先，在命令提示符窗口输入 ipconfig /release，执行后将释放所有适配器或特定适配器的当前 DHCP 配置并丢弃 IP 地址配置，接着输入命令 ipconfig /renew，执行后将重新从 DHCP 服务器上获取新的 IP 地址。

```
C:\>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : C48BB8774EBC4E0
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Eth
ernet NIC
        Physical Address. . . . . . . . . : 00-E0-6F-4F-F9-40
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.178
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 202.96.128.86
                                            202.96.128.166
```

图 9-6　查看详细的网络配置信息

7. 网卡地址及协议列表工具——getmac

getmac 命令用于返回计算机中所有网卡的 MAC 地址，以及每个地址的网络协议列表，既可以应用本地计算机，又可以通过网络获取远程主机或者用户计算机的 MAC 地址等相关信息。

例如，若要获取本地的网卡地址以及协议名称，则在命令提示符窗口中输入 getmac 命令并执行，结果如图 9-7 所示。



```
C:\>getmac

物理地址             传输名称
===================  ==========================================================
00-E0-6F-4F-F9-40    \Device\Tcpip_{04160C34-AB41-43D9-AF60-B7282DC456DB}
```

图 9-7　本地网卡地址以及协议名称

如果要查看 MAC 地址的详细信息，则在命令提示符窗口中输入如下命令：

```
getmac /fo table /nh /v
```

8. 网络协议统计工具——netstat

netstat 程序有助于了解网络的整体使用情况，它可以显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息，可以让用户得知目前共有哪些网络连接正在运行。可以使用 netstat/? 命令来查看一下该命令的使用格式以及详细的参数说明。利用该程序提供的参数功能，可以了解该命令的其他功能信息，例如显示以太网的统计信息，显示所有协议的使用状态，这些协议包括 TCP 协议、UDP 协议、IP 协议等。另外，还可以选择特定的协议并查看其具体使用信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

例如，如果想要了解主机的出口地址、网关地址等信息，则在命令提示符窗口中输入 netstat，按下回车键执行，结果如图 9-8 所示。

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    C48BB8774EBC4E0:2058   61.135.158.12:12320    ESTABLISHED
  TCP    C48BB8774EBC4E0:2796   61.135.158.147:http    CLOSE_WAIT
  TCP    C48BB8774EBC4E0:2797   218.25.41.138:http     CLOSE_WAIT
  TCP    C48BB8774EBC4E0:2798   218.25.41.138:http     CLOSE_WAIT
  TCP    C48BB8774EBC4E0:2799   218.25.41.138:http     CLOSE_WAIT
  TCP    C48BB8774EBC4E0:2800   218.25.41.138:http     CLOSE_WAIT
  TCP    C48BB8774EBC4E0:2801   zz-12-179-a8.bta.net.cn:http  ESTABLISHED
```

图 9-8　netstat 命令信息

9.4.2　硬件工具

1. 物理线缆测试仪

物理线缆测试仪一般指的是现场测试仪，作用是进行布线故障问题诊断，以便工程师和管理员能够在最短的时间内发现布线错误、排除故障。物理线缆测试仪可以分为网络线缆测试仪、网络线缆认证测试仪、网络验证测试仪等几类产品。

如图 9-9 所示是美国福禄克公司推出的一款集多种测试功能于一身的网络测试仪器——MicroScanner Pro 数字式超 5 类电缆分析仪。它专为防止和解决电缆安装问题而设计，可以检测电缆的通断、电缆的连接线序、电缆故障的位置等方面，其显著的特色就是将一系列测试结果直观地反映在显示屏上。

图 9-10 是一款国产的线缆测试仪——TPT-8020A。该款测试仪是一款综合了高级线缆测试和简易网络测试多项功能的手持仪表。具体功能如下：

1）线缆测试

（1）长度测试：满足双绞线、电话线、同轴电缆、普通导线等多种线缆测试要求。

（2）线序测试：显示线序图；可检测是否为屏蔽网线，诊断开路、短路、线序错等故障；检测线缆是否满足 T568A/B 标准要求。

（3）音频寻线：可产生多达四种不同的音频信号，用于在天花板或配线柜中查找线缆。

（4）端口识别：识别端口和插座类型，如以太网、电话等。以太网可以显示速率和双工模式，最高支持 1000Mbps。

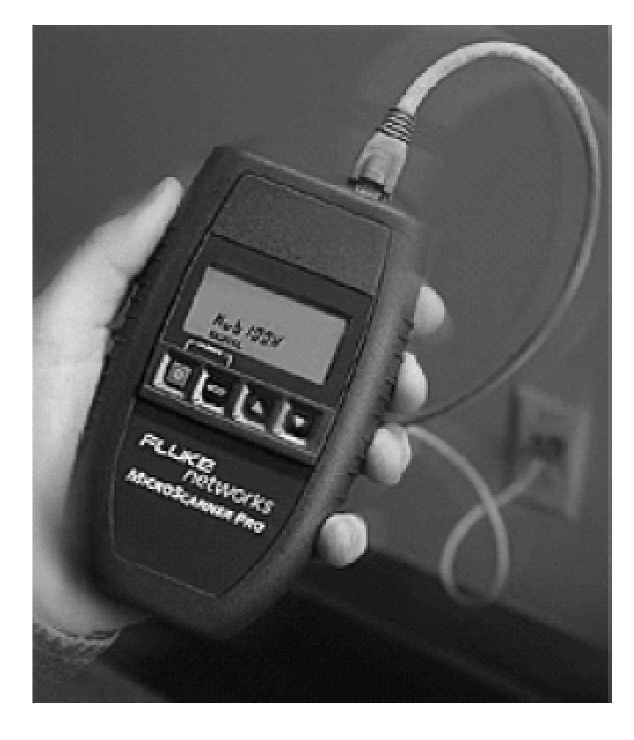


图 9-9　物理线缆测试仪图



图 9-10　TPT-8020A 测试仪

2）网络测试

（1）闪亮端口：闪烁集线器或交换机端口指示灯，帮助确定端口位置。

（2）ping 测试：支持 ping 功能，检测网络丢包等故障。

（3）DHCP 测试：支持 DHCP 自动获取或手动设置 IP 地址。

(4) 网络扫描：检测设定网段中正在使用的主机数量，并显示 IP 地址和 MAC 地址。

2. 网络测试仪

网络测试仪通常也称智能网络测试仪，它将网络管理、故障诊断和网络安装调试等众多功能集中在一个仪器里，它可以通过网桥、路由器很容易地观察整个网络的健康状况，甚至可以诊断出远端网络的问题。测试仪的高级 SNMP 还可以连续获取并不断更新故障网络的信息。网络测试仪可以帮助网络管理人员在较短的时间内对网络的运行情况，以及故障点做出判断。

网络测试仪可以检测 OSI 模型定义的物理层、数据链路层、网络层运行状况，主要适用于局域网故障检测和综合布线施工，用以检测的传输介质通常包括双绞线、同轴电缆和光纤等。网络测试仪的功能涵盖物理层、数据链路层和网络层，主要功能有电缆诊断、线序扫描，拓扑监测、ping IP、端口识别、POE 检测等。

网络测试仪按网络连接方式可以分为无线网络测试仪和有线网络测试仪两类。

(1) 有线网络测试仪

有线网络中常见的传输介质包括双绞线、光纤和同轴电缆。同轴电缆已经很少见了，普遍被使用的是双绞线，光纤是未来网络的发展方向。市场上针对传输介质开发出的网络测试仪，分为光纤网络测试仪和双绞线网络测试仪，光纤网络测试仪并不常用，所以通常所说的网络测试仪都是指双绞线网络测试仪。

如图 9-11 所示为安捷伦 J6800A 网络分析仪。该款产品主要用于数据网络的安装部署、维护与优化，适用于电信运营商的现场安装与维护、企业网络的网络管理与设备制造商研发部门的各类工程技术人员。它既支持集中式的网络故障诊断，又支持分布式网络状况监测，涵盖局域网、广域网、ATM、IP 电话、移动(包括 3G)、NGN 等各类应用。

此外，它可以实现集中式故障定位与分布式监测分析功能。集中式测试具备双端口测试功能，实现 LAN-LAN、LAN-WAN、LAN-ATM 多种组合测试；分布式测试能够同时测量网络中多个测试点的协议与网络性能状况，采集网络数据信息，排查间隙性与深层网络问题，全方位管理与监测网络。

(2) 无线网络测试仪

无线网络测试仪主要是针对无线路由和 AP 进行检测，可以排查出无线网络中连接的终端和无线信号强度，进而能有效地管理网络中的节点，增强网络安全性。该类产品技术还不是很成熟，随着无线网络的推广，无线网络测试仪也会越来越受网络管理的重视，成为一种重要的检测工具。

如图 9-12 所示的 WP150 无线网络测试仪，是一款多功能无线网络故障诊断和维护工具。它可以帮助无线网络安装商和使用者快速识别、查看和配置无线网络的重要信息并发现潜在的故障现象。



图 9-11 安捷伦 J6800A 网络测试仪



图 9-12 WP150 无线网络测试仪

3. 协议分析仪

协议分析仪是能够捕获网络报文的设备，能够找出网络中潜在的问题。协议分析仪在功能和设计方面有很多不同，有些只能分析一种协议，而另一些能够分析几百种协议。一般情况下，大多数的协议分析仪至少能够分析以太网、TCP/IP、IPX、DECNet 等协议。

协议分析仪通常是软硬件的结合，通常使用专用硬件或设置为专用方式的网卡实施对网络中的数据捕捉。捕获在网络中传输的数据信息的方法称为 sniffing(嗅探)。

协议分析仪的工作从原理上分为数据采集和协议分析两个部分。对这两部分的工作从实现的形式上来说有以下常见的几种形式。

(1) 纯软件的协议分析系统

大多数的纯软件协议分析仪可以使用普通网卡来完成简单的数据采集工作，这就是使用率最多的"协议分析软件＋PC 网卡"。本来协议分析工作就是基于软件分析的工作，所以再高端的协议分析仪其软件部分也是由计算机平台实现的。

(2) 基于"笔记本＋数据采集箱"的便携式协议分析仪

这种方式与上述采用"协议分析软件＋PC 网卡"的主要区别就是专用的数据采集系统。在相对复杂和高速的网络链路上，要想全线速地捕捉或更有效地进行实时数据过滤，采用专用的数据采集方式是必须的。

(3) 手持式综合协议分析仪

从协议分析仪发展的角度来说，网络维护人员越来越需要使用功能强大并能将多种网络测试手段集于一身的综合式测试分析手段，典型的协议分析仪上的功能延展就是加入网管功能、自动网络信息搜集功能、智能的专家故障诊断功能，并且移动性能要有效。这种综合的协议分析仪或者说是综合的网络分析仪成为了当今网络维护测试仪的主要发展趋势，像 Fluke 的 OptiView INA 自上市以来在网络现场分析、故障诊断、网络维护中得到了相当广泛的应用和发展。

(4) 分布式协议分析仪

随着网络维护规模的加大，网络技术的变化，网络关键数据的采集也越来越困难。有时为了分析和采集数据，必须在异地同时进行采集，于是将协议分析仪的数据采集系统独立开来，能安置在网络的不同地方，由能控制多个采集器的协议分析仪平台进行管理和数据处理，这种应用模式就促生了分布式协议分析仪。

图 9-13 为 OptiView 集成式网络分析仪，是一款硬件和软件的集成式解决方案，可以提供对整个企业网络的便携式或分布式的透视能力。OptiView 将协议分析、流量分析和网络搜索三大功能集于一身，提供了全新的快速、易用、深层透视、有助于优化 WAN、LAN 和 WLAN 性能的网络分析解决方案。该分析仪包括一个高性能协议分析仪，一个快速电缆测试仪，一个 RMONv2 探头。

图 9-13　Optiview 集成式网络分析仪

9.5 常见的网络故障及解决方法

9.5.1 工作站故障

1. IP 地址冲突

使用 TCP/IP 协议的每台计算机必须有自己独立的 IP 地址，有了 IP 地址才能与网络上的其他主机进行通信。一般情况下，IP 地址配置不正确，主要表现为 IP 地址冲突。如下几种情况可以造成 IP 地址冲突：

(1) 用户对 TCP/IP 并不了解，不知道 IP 地址、子网掩码、默认网关等参数如何设置，有时用户不是从管理员处得到上述参数的信息，或者是用户无意修改了这些信息。

(2) 管理员或用户根据管理员提供的上述参数进行设置时，由于失误造成参数输错。

(3) 维修调试时，维修人员使用临时 IP 地址所致。

(4) 故意窃用他人的 IP 地址。

2. 子网掩码设置不正确

子网掩码是一个 32 位地址，是与 IP 地址结合使用的一种技术。它的主要作用有两个：一是用于屏蔽 IP 地址的一部分以区别网络标识和主机标识，并说明该 IP 地址是在局域网上，还是在远程网上；二是用于将一个大的 IP 网络划分为若干小的子网络。

在同一网段中的计算机应该具有相同的子网掩码。如果子网掩码不同，就算是位于同一个网段的计算机也不可能通信。所以，如果同一网段的计算机之间不能通信，除了 IP 地址必须正确以外，子网掩码也必须相同。

3. 没有安装网络协议

网络协议是网络上所有设备之间通信规则的集合，它规定了通信时信息必须采用的格式和这些格式的意义。

不同的计算机之间必须使用相同的网络协议才能进行通信。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。常见的协议有：TCP/IP 协议、IPX/SPX 协议、NetBEUI 协议等。用户如果访问 Internet，则必须在网络协议中添加 TCP/IP 协议。

TCP/IP 协议规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式以及传送方式。TCP/IP 是 Internet 的基础协议，也是一种数据打包和寻址的标准方法。

4. 网关没有设置或设置不正确

网关是一个网络通向其他网络的 IP 地址，要实现这两个网络之间的通信，必须通过网关。如果网络 A 中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络 B 的网关，网络 B 的网关再转发给网络 B 的某个主机。所以，只有设置好网关的 IP 地址，TCP/IP 协议才能实现不同网络之间的相互通信。

5. DNS 地址设置不正确

DNS 设置不正确，就不能对 IP 地址进行解析，也就无法使用域名进行网络访问，而只有使用 IP 地址进行网络访问。如果在访问网站时，在浏览器中输入 IP 地址可以访问某一

网站，却无法通过域名进行访问，在这种情况下，首先检查是否设置了 DNS 地址，或确认地址是否正确。如果 DNS 地址无问题，则可能是网站的 DNS 服务器出了问题。

9.5.2 服务器故障

1. 服务器常见的故障及排除方法

(1) 服务被中止

由于用户过多，内存占用过大等原因，服务器上的服务被中止，这时可以在服务器上检查出该项服务是否被中止。若被中止，则重新启动该项服务即可。

(2) 流量问题

由于服务器需要为大量的用户提供大量的服务，流量过大或大量的错误帧的出现，都有可能产生拥塞现象甚至是广播风暴，导致服务器的性能下降甚至死机。通常如果利用率过高(平均值大于 40%，瞬时峰值高于 60%)，则网络负荷就过重了。如果利用率很高，其持续峰值超过 60%，而平均碰撞小于 10%，那么网络就饱和了，这种情况可以利用网络分析仪等工具对服务器网卡的流量和数据帧进行检测。同时可以分析异常流量来自何处，以便采取相应的措施。

(3) 系统资源不足

服务器上提供的服务越多，服务器对设置和硬件要求也就越高。若服务器的软、硬件资源不能满足要求，或由于计算机蠕虫等病毒抢占计算机资源，也会造成计算机性能下降或网络故障。如果是前一个原因，其解决的方法是提升软、硬件设备的能力，或对系统资源重新设置。例如，加大服务器的内存、加大缓冲内存和删除不必要的临时文件，这在一定程度上可以缓解或解决系统对内存的要求。若是后者，查杀病毒并重新启动服务即可，但要以防止病毒的入侵为主，须安装防病毒的软件。

(4) 服务器软件故障

服务器软件故障是在服务器故障中占有比例最高的部分，约占 70%。导致服务器出现软件故障的原因有很多，最常见的是服务器 BIOS 版本太低、服务器的管理软件或服务器的驱动程序有 BUG、应用程序有冲突及人为造成的软件故障。服务器软件设置不当也可能造成网络故障。例如，每一个网络服务都要有相应的服务端口，如果其端口被其他服务占用，则该服务就不能正常运行。这种情况，一般可以通过改变端口的设置来解决。另外，客户机的浏览器本身有故障或配置不正确也会导致连接不到服务器，这种情况可以通过重新安装浏览器来解决。

(5) 管理方面的问题

服务器由于管理不善造成一些问题，如用户的账户和安全设置方面的潜在问题，服务权限配置不当或限制某些服务等问题，这些问题需要通过重新配置来解决。

2. 服务器故障排除的基本原则

1) 尽量恢复系统默认配置

(1) 硬件配置：去除第三方厂商备件和非标配备件。

(2) 资源配置：清除 CMOS，恢复资源初始配置。

(3) BIOS、F/W、驱动程序：升级最新的 BIOS、F/W 和相关驱动程序。

(4) TPL：扩展的第三方的 I/O 卡应属于该机型的硬件兼容列表(TPL)。

2）从基本到复杂

（1）系统上从个体到网络：首先将存在故障的服务器独立运行，待测试正常后再接入网络运行，观察故障现象变化并处理。

（2）硬件上从最小系统到现实系统：从可以运行的硬件开始，逐步扩展到现实系统为止。

（3）软件上从基本系统到现实系统：从基本操作系统开始，逐步扩展到现实系统为止。

3）交换对比

（1）在最大可能相同的条件下，交换操作简单效果明显的部件。

（2）交换 NOS 载体，即交换软件环境。

（3）交换硬件，即交换硬件环境。

（4）交换整机，即交换整体环境。

3. 服务器故障排除需要收集的信息

（1）服务器信息：机器型号（P/N）、机器序列号（S/N）、BIOS 版本、是否增加其他设备、硬盘如何配置（是否做阵列，阵列级别）、安装什么操作系统及版本。

（2）故障信息：在 POST 时，屏幕显示的异常信息、服务器本身指示灯的状态、报警声和 BEEP CODES、NOS 的事件记录文件、Events Log 文件。

（3）确定故障类型和故障现象：开机无显示、上电自检阶段故障、安装阶段故障和现象、操作系统加载失败、系统运行阶段故障。

9.5.3 交换机故障

交换机故障一般可以分为硬故障和软故障两大类。

1. 硬故障

硬故障主要指交换机电源、背板、模块、端口、线缆等部件的故障，可以分为以下几类。

（1）电源故障

由于外部供电不稳定，或者电源线路老化或者雷击等原因导致电源损坏或者风扇停止，从而不能正常工作。由于电源缘故而导致机内其他部件损坏的事情也经常发生。

通常面板上的 Power 指示灯是绿色的，就表示是正常的；如果该指示灯灭了，则说明交换机没有正常供电。这类问题很容易发现，也很容易解决，同时也是最容易预防的。

针对这类故障，首先应该做好外部电源的供应工作，一般通过引入独立的电力线来提供独立的电源，并添加稳压器来避免瞬间高压或低压现象。如果条件允许，可以添加 UPS 来保证交换机的正常供电，有的 UPS 提供稳压功能，而有的没有，选择时要注意。在机房内设置专业的避雷措施，来避免雷电对交换机的伤害。现在有很多做避雷工程的专业公司，实施网络布线时可以考虑。

（2）端口故障

这是最常见的硬件故障，无论是光纤端口还是双绞线的 RJ-45 端口，在插拔接头时一定要小心。如果不小心把光纤插头弄脏，可能导致光纤端口污染而不能正常通信。带电插拔接头从理论上讲是可以的，但是这样也无意中增加了端口的故障发生率。在搬运时不小心，也可能导致端口物理损坏。如果购买的水晶头尺寸偏大，插入交换机时，也容易破坏端口。此外，如果接在端口上的双绞线有一段暴露在室外，万一这根电缆被雷电击中，就会导致所

连交换机端口被击坏，或者造成更加不可预料的损伤。

一般情况下，端口故障是某一个或者几个端口损坏。所以，在排除了端口所连计算机的故障后，可以通过更换所连端口来判断其是否损坏。遇到此类故障，可以在电源关闭后，用酒精棉球清洗端口。如果端口确实被损坏，那就只能更换端口了。

（3）模块故障

交换机是由堆叠模块、管理模块（也叫控制模块）、扩展模块等很多模块组成的。虽然这些模块发生故障的几率很小，不过一旦出现问题，就会遭受巨大的经济损失。如果插拔模块时不小心，或者搬运交换机时受到碰撞，或者电源不稳定等情况，都可能导致此类故障的发生。

在排除此类故障时，首先应确保交换机及模块的电源正常供电，然后检查各个模块是否插在正确的位置上，最后检查连接模块的线缆是否正常。在连接管理模块时，还要考虑它是否采用规定的连接速率，是否有奇偶校验，是否有数据流控制等因素。连接扩展模块时，需要检查是否匹配通信模式。当然，如果确认模块有故障，解决的方法只有一个，那就是应当立即联系供应商处理。

（4）背板故障

交换机的各个模块都是接插在背板上的。如果环境潮湿，电路板受潮短路，或者元器件因高温、雷击等因素而受损，都会造成电路板不能正常工作。如果散热性能不好或环境温度太高，将导致机内温度升高而使元器件烧坏。

在外部电源正常供电的情况下，如果交换机的各个内部模块都不能正常工作，那就可能是背板坏了，遇到这种情况即使是电器维修工程师，恐怕也无计可施，唯一的办法就是更换背板了。

（5）线缆故障

从理论上讲，这类故障不属于交换机本身的故障，但在实际使用中，电缆故障经常导致交换机系统或端口不能正常工作，所以这里也把这类故障归入交换机硬件故障。比如接头接插不紧，线缆制作时顺序排列错误或者不规范，线缆连接时应该用交叉线却使用了直连线，光缆中的两根光纤交错连接，错误的线路连接导致网络环路等。

从上面的几种硬件故障来看，机房环境不佳极易导致各种硬件故障，所以在建设机房时，必须先做好防雷接地及供电电源、室内温度、室内湿度、防电磁干扰、防静电等环境的建设，为网络设备的正常工作提供良好的环境。

2. 软故障

交换机的软故障是指系统及其配置上的故障，它可以分为以下几类。

（1）系统错误

交换机系统是硬件和软件的结合体。在交换机内部有一个可刷新的只读存储器，它保存的是这台交换机所必需的软件系统。由于设计的原因，可能会存在一些漏洞，在某些条件下，会导致交换机满载、丢包、错包等情况的发生。

对于此类问题，需要养成经常浏览设备厂商网站的习惯，如果有新的系统推出或者新的补丁，请及时更新。

（2）配置不当

由于对交换机的性能等技术指标不熟悉可能会导致配置错误的出现。比如 VLAN 划分不当导致网络不通、端口被错误地关闭、交换机和网卡的模式不匹配等原因。这类故障有

时很难发现，如果不能确保配置的正确性，最好先恢复出厂的默认配置，然后再一步一步地配置。

在配置之前先阅读说明书是好的习惯之一。每台交换机都有详细的安装手册、用户手册，深入到每类模块都有详细的讲解。如果还有不清楚之处，就需要向供应商的工程师咨询后再做具体配置。

9.5.4 路由器故障

在路由器出现的故障中，大体可以分为两类：一类是硬故障，另一类是软故障。

1. 硬故障

常见的硬故障通常表现在硬件上，一般有以下几种。

(1) 系统不能正常加电

表现为当打开路由器的电源开关时，路由器前面板的电源灯不亮，风扇不转。这时要重点检查电源系统，看供电插座是否有电，电压是否在规定的范围内。如果供电正常，应该检查电源线是否完好，接触是否牢靠，必要时可以换一根，如果还不行，可判定问题应该出在路由器的电源上。先检查路由器电源的保险是否完好，若烧了应该更换，若还不行只好送修。

(2) 部件损坏

这类情况在硬件故障中是比较常见的，这里的部件往往是接口卡，表现为当把有问题部件插到路由器中时，系统其他部分都工作正常，但无法正确识别有问题的部件，这时往往是因为部件本身有问题。还有一种情况，就是部件可以被正确识别，但做完正确配置后，接口就是不能正常工作，这往往是因为存在物理故障。要确认以上这两种情况，最好用相同型号的好的部件替换怀疑有问题的部件，就可以确认问题是否存在了。

(3) 系统软件损坏

这种故障似乎应该归入软件故障，但由于这种情况往往是路由器本身存在的问题，且与硬件紧密相关，所以不妨把它归类于此。以 Cisco 的路由器为例，如果路由器开机后总是进入 rmon 状态，这往往说明系统软件 IOS 存在问题，不妨将 IOS 重新写一遍。

(4) 其他

这里所要提到的是这样一些情况，有时在对系统软件进行升级时，发现系统无论怎样也不能完成升级。这时不妨检查一下所要升级的软件的大小是否超过了路由器的 NVRAM 的容量。如果超过了，则无论如何也无法完成升级，这时应该先扩充 NVRAM 的容量，再升级系统软件。

2. 软故障

(1) 功能无法实现

有些时候，用户要做某些特定的配置(如 NAT)，反复检查后，确认配置正确，可相应的功能就是实现不了。这时先不要怀疑设备有问题，最好找一找系统软件的版本号，并查找相关的说明，看一看所使用的软件的版本是否支持这个功能。因为路由器的系统软件往往有许多版本，每个版本支持不同的功能。如果当前的软件版本不支持这个功能，那就应该找到相应的软件，先进行升级。

(2) 网络规划存在问题

有些时候，配置似乎没有问题，可路由器就是不能正常工作，或者工作状态不稳定，总出

现一些莫名其妙的问题。这时先不要急着反复调试，不妨回过头来看看用户的网络规划，看看是不是有问题。例如是不是有重复使用的网段、网络掩码的计算是否正确等。

（3）配置问题

这种问题是最常见的，就是配置的确存在问题，例如线路两端路由器的参数不匹配或参数错误等。这种情况只要认真细致地查找，总可以解决。

3. 路由器故障的排除

1）串口故障排除

串口出现连通性疑问时，为了排除串口故障，一般是从 show interface serial 命令开始，分析它的屏幕输出报告内容，找出疑问之所在。串口报告的开始提供了该接口状态和线路协议状态。接口和线路协议的可能组合有以下几种：

（1）串口运行、线路协议运行，这是完全的工作条件。该串口和线路协议已经原始化，并正在交换协议的存活信息。

（2）串口运行、线路协议关闭，这说明路由器与提供载波检测信号的设备连接，表明载波信号出现在本地和远程的调制解调器之间，但没有正确交换连接两端的协议存活信息。可能的故障发生在路由器配置问题、调制解调器操作问题、租用线路干扰或远程路由器故障、数字式调制解调器的时钟问题、通过链路连接的两个串口不在同一子网上，所有这些都会出现这个报告。

（3）串口和线路协议都关闭，可能是电信部门的线路故障、电缆故障或者是调制解调器故障。

（4）串口可管理功能关闭和线路协议关闭，这种情况是在接口配置中输入了 shutdown 命令，通过输入 no shutdown 命令即可打开。接口和线路协议都运行的状况下，虽然串口链路的基本通信建立起来了，但仍然可能由于信息包丢失和信息包不正确时会出现许多潜在的故障问题。正常通信时，接口输入或输出信息包不应该丢失，或者丢失的量非常小，而且不会添加。如果信息包丢失有规律性添加，表明通过该接口传输的通信量超过接口所能处理的通信量。处理的办法是添加线路容量。查找其他原因引发的信息包丢失，查看 show interface serial 命令的输出报告中的输入输出保持队列的状态。当发觉保持队列中信息包数量达到了信息的最大允许值时，可以添加保持队列配置的大小。

2）以太接口故障排除

以太接口的典型故障是：带宽的过分运用、碰撞冲突次数频繁、运用不兼容的帧类型等。运用 show interface ethernet 命令可以查看该接口的吞吐量、碰撞冲突、信息包丢失、和帧类型的有关内容等。通过查看接口的吞吐量可以检测网络的运用。如果网络广播信息包的百分比很高，网络性能开始下降。光纤网转换到以太网段的信息包可能会淹没以太口。若互联网发生这种情况，可以采用优化接口的方法，即在以太接口运用 no ip route-cache 命令，禁用高速转换，并且调整缓冲区和保持队列。

当两个接口试图同时传输信息包到以太电缆上时将发生碰撞。以太网要求冲突次数很少，不同的网络要求是不同的，一般情况发觉冲突每秒有 3、5 次就应该查找冲突的原因了。碰撞冲突产生拥塞，碰撞冲突的原由通常是由于敷设的电缆过长、过分运用。以太网络在物理设计和敷设电缆系统管理方面应有所考虑，超规范敷设电缆可能引起更多的冲突发生。如果接口和线路协议报告运行状态，并且节点的物理连接都完好，可是不能通信。引起此问

题的原因也可能是两个节点运用了不兼容的帧类型，处理的办法是重新配置，使之运用相同帧类型。如果要求运用不同帧类型的同一网络的两个设备互相通信，可以在路由器接口运用子接口，并为每个子接口指定不同的封装类型。

3）异步通信口故障排除

互联网络的运行中，异步通信口的任务是为用户提供可靠服务，但又是故障多发部位。主要的问题是，在通过异步链路传输基于 LAN 通信量时，将丢失的信息包的量降至最少。异步通信口故障一般的外部因素是：拨号链路性能低，电话网交换机的连接质量问题，调制解调器的配置情况。

当异步通信口出现故障时，首先要检查链路两端运行的调制解调器。连接到远程 PC 机端口调制解调器的问题不太多，因为每次生成新的拨号时通常都初始化调制解调器，运用大多数通信程序都能在发出拨号命令之前发送适当的配置字符串；连接路由器端口的问题较多，这个调制解调器通常等待来自远程调制解调器的连接，连接之前，并不接收配置字符串。

如果调制解调器丢失了它的配置，应采用一种方案来初始化远程调制解调器。基本的办法是运用可通过前面板配置的调制解调器，另一种方法是将调制解调器接到路由器的异步接口，建立反向 telnet，发送设置命令配置调制解调器。

show interface async 命令、show line 命令是诊断异步通信口故障运用最多的工具。在 show interface async 命令输出报告中，接口状态报告关闭的唯一的情况是接口没有设置封装类型。线路协议状态显示与串口线路协议显示相同。show line 命令显示接口接收和传输速度设置以及 EIA 状态显示。show line 命令可以认为是接口命令（show interface async）的扩展。

确定异步通信口故障一般可用下列步骤：检查电缆线路质量，检查调制解调器的参数配置，检查调制解调器的连接速度，检查 rxspeed 和 txspeed 能不能与调制解调器的配置匹配，通过 show interface async 命令和 show line 命令查看端口的通信状况，从 show line 命令的报告检查 EIA 状态显示，检查接口封装，检查信息包丢失及缓冲区丢失情况。

9.6 本章小结

本章介绍了网络故障的诊断与网络维护的相关知识，重点是网络故障产生的原因、故障诊断的原理，以及故障排除的步骤等内容。首先介绍了网络故障诊断的目的、故障产生的原因、排除的方法和步骤，然后介绍了网络故障的分类，以及故障分层检查的原理。接着介绍了网络故障诊断的常用软、硬件工具。最后介绍了常见网络故障及排除方法。

分层检查指导故障分别定位于物理层、数据链路层、网络层、传输层和应用层，分段诊断也是常用的方法之一，即把故障定位于某一网段的设备上。

习　题　9

一、选择题

1. 将多个子网断开后作为各自独立的子网进行测试属于（　　）检查。

   A. 整体　　B. 分层　　C. 分段　　D. 其他

2. 设备电缆出现的问题属于(　　)问题。

A. 物理层　B. 数据链路层　C. 网络层　D. 应用层

3. IP地址发生了冲突以后可以使用(　　)命令来查找非法使用者地址的主机。

A. netsta　B. winipcfg　C. tracert　D. nbtstat

4. 在浏览器的地址栏中输入IP地址可以访问网站,而输入域名则不能访问网站,这种情况可能是(　　)。

A. IP地址设置错误　B. DNS设置错误

C. 网关设置错误　D. 子网掩码设置错误

5. ping命令失败了,这时ping命令会显示出错信息,这种错误信息通常是(　　)。

A. network unreachable　B. unknow host

C. no answer　D. 以上都正确

6. 由于OSI各层功能具有相对独立性,所以按层排查故障可以有效发现和隔离故障,通常逐层分析和排查的策略在具体实施时(　　)。

A. 从低层开始　B. 从高层开始

C. 从中间开始　D. 根据具体情况选择

7. 在各种设备的故障问题中,比较普遍的问题是(　　)。

A. 配置问题　B. 硬件问题

C. 规划设计问题　D. 黑客攻击

二、简答题

1. 故障排除的基本步骤是什么?
2. OSI协议各层的功能是什么?容易产生什么问题?
3. 网卡的工作原理是什么?故障有哪些?
4. 如何选择服务器?服务器的故障通常有哪些?
5. 交换机的故障有哪些?
6. 路由器的技术指标有哪些?其故障有哪些?
7. 网络测试工具有哪些?

参 考 文 献

[1] 陶洋.网络系统管理与控制[M]. 北京：人民邮电出版社，2007.

[2] 王群.非常网管[M]. 北京：人民邮电出版社，2006.

[3] 唐树才.计算机网络管理[M]. 北京：清华大学出版社，2002.

[4] 李振银.网络管理与维护[M]. 北京：中国铁道出版社，2005.

[5] 刘晓辉，杨兴明.中小企业网络管理员实用教程[M]. 北京：科学出版社，2004.

[6] 骆耀祖，刘永初，李强. Cisco 路由器实用技术教程[M]. 北京：电子工业出版社，2002.

[7] 褚建立，刘彦舫.网络综合布线实用技术[M]. 北京：清华大学出版社，2004.

[8] 王淑江等.网络管理[M]. 北京：机械工业出版社，2007.

[9] 冯英健.网络营销基础与实践[M]. 北京：清华大学出版社，2007.

[10] 雷震甲.计算机网络管理[M]. 北京：人民邮电出版社，2009.

[11] 甘刚.网络设备配置与管理[M].北京：清华大学出版社，2007

[12] ISO/IEC 17799：2000，Information technology——Code of Practice for information security management[S].Geneva：International Organization for Standardization，2000.

[13] http://www.ruijie.com.cn/htmls/3-23/35peizhi

[14] http://www.yesky.com/20020522/1612512.shtml

21 世纪高等学校数字媒体专业规划教材

ISBN	书　名	定价(元)
9787302224877	数字动画编导制作	29.50
9787302222651	数字图像处理技术	35.00
9787302218562	动态网页设计与制作	35.00
9787302222644	J2ME 手机游戏开发技术与实践	36.00
9787302217343	Flash 多媒体课件制作教程	29.50
9787302208037	Photoshop CS4 中文版上机必做练习	99.00
9787302210399	数字音视频资源的设计与制作	25.00
9787302201076	Flash 动画设计与制作	29.50
9787302174530	网页设计与制作	29.50
9787302185406	网页设计与制作实践教程	35.00
9787302180319	非线性编辑原理与技术	25.00
9787302168119	数字媒体技术导论	32.00
9787302155188	多媒体技术与应用	25.00
9787302235118	虚拟现实技术	35.00
9787302234111	多媒体 CAI 课件制作技术及应用	35.00
9787302238133	影视技术导论	29.00
9787302224921	网络视频技术	35.00
9787302232865	计算机动画制作与技术	39.50

以上教材样书可以免费赠送给授课教师，如果需要，请发电子邮件与我们联系。

教学资源支持

敬爱的教师：

感谢您一直以来对清华版计算机教材的支持和爱护。为了配合本课程的教学需要，本教材配有配套的电子教案(素材)，有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案(素材)，希望有助于教学活动的开展。

相关信息请拨打电话 010-62776969 或发送电子邮件至 weijj@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页(http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn)上查询和下载。

如果您在使用本教材的过程中遇到了什么问题，或者有相关教材出版计划，也请您发邮件或来信告诉我们，以便我们更好地为您服务。

地址：北京市海淀区双清路学研大厦 A 座 708　　计算机与信息分社魏江江　收
邮编：100084　　电子邮件：weijj@tup.tsinghua.edu.cn
电话：010-62770175-4604　　邮购电话：010-62786544

《网页设计与制作(第 2 版)》目录

ISBN 978-7-302-25413-3
梁 芳 主编

图书简介：

Dreamweaver CS3、Fireworks CS3 和 Flash CS3 是 Macromedia 公司为网页制作人员研制的新一代网页设计软件，被称为网页制作"三剑客"。它们在专业网页制作、网页图形处理、矢量动画以及 Web 编程等领域中占有十分重要的地位。

本书共 11 章，从基础网络知识出发，从网站规划开始，重点介绍了使用"网页三剑客"制作网页的方法。内容包括了网页设计基础、HTML 语言基础、使用 Dreamweaver CS3 管理站点和制作网页、使用 Fireworks CS3 处理网页图像、使用 Flash CS3 制作动画和动态交互式网页，以及网站制作的综合应用。

本书遵循循序渐进的原则，通过实例结合基础知识讲解的方法介绍了网页设计与制作的基础知识和基本操作技能，在每章的后面都提供了配套的习题。

为了方便教学和读者上机操作练习，作者还编写了《网页设计与制作实践教程》一书，作为与本书配套的实验教材。另外，还有与本书配套的电子课件，供教师教学参考。

本书可作为高等院校本、专科网页设计课程的教材，也可作为高职高专院校相关课程的教材或培训教材。

目 录：